

ValiCert[®] Validator Suite[™]

Installation and Configuration Guide

Version 3.2



© 2000 ValiCert, Inc. All rights reserved. ValiCert and the ValiCert logo are registered trademarks of ValiCert, Inc. Powering e-Transactions, ValiCert Digital Receipt Solutions, ValiCert Enterprise VA Suite, ValiCert Enterprise VA, ValiCert Certificate VA Suite, ValiCert Certificate VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Web Server Validator, ValiCert E-Mail Validator, ValiCert Address Book Validator, ValiCert Browser Validator, ValiCert Validator Toolkit, ValiCert Receipt Notary, ValiCert Receipt Vault, ValiCert Receipt Toolkit, ValiCert SecureTransport, ValiCert SecureTransport/File, and ValiCert SecureTransport/XML and Stateful Validation are trademarks of ValiCert, Inc. ValiCert Global VA Service and ValiCert Receipt Service are service marks of ValiCert, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

ValiCert, Inc.
1215 Terra Bella Avenue
Mountain View, CA 94043

Part Number: DCU-B-VSIG-0320E

Revision: 0215-1

Table of Contents

Preface

1 Introduction

E-Mail Validator	1
Receiving Signed E-Mail	1
Sending Signed E-Mail.	2
Reading E-Mail Offline	2
Address Book Validator	2
Web Server Validator for Microsoft IIS.	3
Web Server Validator for Netscape	3
Browser Validator.	4

2 Getting Started

E-Mail Validator Requirements	5
Address Book Validator Requirements	5
Web Server Validator (Microsoft IIS) Requirements	6
Web Server Validator (Netscape) Requirements.	7
Browser Validator Requirements	8
Installing the Validator Suite on Windows NT	9
Modifications to obj.conf File for the Web Server Validator for Netscape	
19	
Installing the Web Server Validator for Netscape on UNIX	19

3 Configuring the E-Mail Validator

Configuring the E-Mail Validator	21
Creating the CRL Initialization File.	24

Adding Trusted Root Certificates	25
Viewing CA Certificates	28
 4 Using the E-Mail Validator	
Starting and Stopping the E-Mail Validator	31
Sending Signed E-Mail Messages	31
Receiving E-Mail	33
Reading E-Mail	34
Revoked Certificates	34
Unknown Issuers	36
Certificates with Unknown Status	36
 5 Using the Address Book Validator	
Starting the Address Book Validator	39
Stopping the Address Book Validator	40
Opening the Main Dialog box	40
Configuring the Address Book Validator	41
Opening the Preferences Dialog Box	42
Configuring the Activity Log	42
Configuring Alert Settings	44
Configuring Connection Settings to Proxy Server	46
Configuring Your Address Books	48
Configuring Validation Settings	49
Validating Certificates	50
Viewing Certificate Status	51
Adding Trusted Root Certificates	53
Sharing Contacts Address Book	57
Creating the CRL Initialization File	58
 6 Using Validator for Microsoft IIS	
Configuring Your Web Server	61
Customizing the Error Page	62

Using CRLs for Validation	62
Editing the Configuration File	63
Using the Web Server Validator	66
7 Using Validator for Netscape Server	
Editing the Configuration File	67
Configuring Validator to use CRLs	71
Configuring Validation Caches	73
Configuring the CRL Cache	73
Configuring the Validation Response Cache	74
Customizing Validator Output	75
Using the Web Server Validator	76
8 Using the Browser Validator	
Validating Certificates	80
Using CRLs to Validate Certificates	82
A Troubleshooting	
Email Validator	85
Web Server Validator for Microsoft IIS	86
Web Server Validator for Netscape Enterprise Server	87

Index

Preface

About This Guide

This manual describes the installation, configuration, and administration of the ValiCert Validator Suite.

Audience

This guide is intended for the user (often the system or network administrator) who is responsible for installing, configuring, and maintaining the ValiCert Validator Suite. The reader fits one of the following profiles, or has equivalent background or knowledge:

- ❖ Customers with technical networking background and experience.
- ❖ System administrators who are familiar with the fundamentals of digital certificates and validation.
- ❖ System administrators who are responsible for installing and configuring software packages.

Organization of This Guide

This guide is organized as follows:

Section	Description
Introduction	Provides an overview of the ValiCert Validator Suite and information about installing it.
Getting Started	Provides information about installing the Validator Suite components.
Configuring the E-Mail Validator	Describes how to configure the ValiCert E-Mail Validator after you have installed the E-Mail Validator.
Using the E-Mail Validator	Describes how to start and stop the add-in, and how to use the e-mail add-in features when sending, reading, and receiving e-mail messages with Microsoft Outlook.
Using the Address Book Validator	Describes how to use and configure the Address Book Validator.
Using Validator for Microsoft IIS	Describes how to configure the Web Server Validator for the Microsoft Internet Information Server.
Using Validator for Netscape Server	Describes how to configure the Web Server Validator for the Netscape Enterprise Server.
Using the Browser Validator	Describes how to configure Internet Explorer to use the Browser Validator and how the browser informs you of the certificate validation status.
Troubleshooting	Provides solutions to problems encountered while using the Validators.

Typographical Conventions

The following typographical conventions are used in this guide to help you locate and identify information:

Italic text is used for emphasis and book titles.

Bold text identifies menu names, menu options, items you can click on the screen, and keyboard keys.

`Courier font` identifies commands you enter at the command line, file names, folder names, and text that either appears on the screen or that you are required to type in.

The base directory that houses all of the components of the Validator Suite is referred to as <VCInstallDir>. The actual location depends on where you install Validator Suite.



NOTE: Notes provide significant, helpful information about a feature, operation, or procedure.

ValiCert Documentation

- ❖ ValiCert Enterprise VA™ Installation and Administration Guide
- ❖ ValiCert VA Publisher™ Installation and Administration Guide
- ❖ ValiCert Validator Suite™ Installation and Configuration Guide
- ❖ ValiCert Validator Toolkit™ Programmer's Guide

Technical Support

ValiCert provides debugging assistance, integration assistance and general customer support. Please contact us through one of the following methods:

- ❖ Email: support@valicert.com
- ❖ Telephone: +1.650.567.5469
- ❖ Fax: +1.650.254.2148

When you contact us, we would appreciate your sending us as much detailed information as possible regarding your:

- ❖ Network
- ❖ Platform
- ❖ Specific problem and how to reproduce it.

Credits



This product contains encryption software from RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. All Rights Reserved.



This product includes portions of SSLeay software written by Eric Young (eyay@mincom.oz.au). Copyright (C) 1995-1997 Eric Young. All rights reserved. This product includes software written by Tim Hudson (tjh@mincom.oz.au).



This product includes software from Netscape Communications Corp. Copyright (C) 1997 Netscape Communications Corp. All rights reserved.

Introduction

This section provides an overview of the ValiCert® Validator™ Suite. The Validators are plug-ins that add validation capability to various applications. The Validator Suite works in conjunction with ValiCert's VA products. To add validation capabilities to your applications, you must have access to a Validation Authority (VA). This can be the ValiCert Global VA Service™, a ValiCert Enterprise VA™, or a ValiCert Certificate VA™.

The Validator Suite is comprised of the following:

- ❖ E-Mail Validator
- ❖ Address Book Validator
- ❖ Web Server Validator for Microsoft IIS
- ❖ Web Server Validator for Netscape
- ❖ Browser Validator

E-Mail Validator

The ValiCert E-Mail Validator is a Microsoft Outlook Add-In module that lets you check the status of digital certificates used to sign S/MIME email. You can also use the module to “piggyback” certificate validation proof when sending signed e-mail with Outlook. This eliminates the need for message recipients to check the revocation status of the certificate you used to sign the message.

Receiving Signed E-Mail

When you receive a signed message, the Validator checks if the message is an S/MIME signed message. If it is, the Validator extracts the signing certificate from the message and queries a VA to determine whether the certificate has been revoked. This process is carried out for all signed e-mail messages that you retrieve.

If a signed e-mail message has a ValiCert Freshness Proof™ stamp attached to it, and you have configured the Validator to trust Freshness Proof stamps, the VA is not queried.

If you receive an S/MIME message that has been signed with a revoked certificate, the Validator will display a message box indicating that the message's certificate is invalid.

Sending Signed E-Mail

When you send a signed e-mail, you can include a validation response (a Freshness Proof stamp) from the VA. This saves the recipient(s) from making a network request to the VA upon receiving the message, provided they have their Validator configured to accept the Freshness Proof stamp. The savings are huge if the number of intended recipients is large.

Reading E-Mail Offline

The Validator stores the e-mail message and its validation status in the MAPI store of Outlook 98 and Outlook 2000. When you read a signed message, the Validator retrieves the validation status from the e-mail message. If the certificate used to sign the message has been revoked, the Validator displays a dialog box that provides additional information about the certificate as well as follow-on action for the e-mail message.

Address Book Validator

The ValiCert Address Book Validator application checks the status of digital certificates present in the various certificate data stores of a computer running Windows NT, Windows 95, or Windows 98. The ValiCert Address Book Validator supports the Microsoft Windows Address Book, which stores information such as e-mail addresses and digital certificates. Note that this is not the same as the Microsoft Outlook Personal Address Book or Contacts database.

Web Server Validator for Microsoft IIS

The ValiCert Web Server Validator for Microsoft IIS is a plug-in that ensures that your Microsoft Internet Information Server (IIS) or Personal Web Server (PWS) does not accept invalid certificates during secure web connections. The Validator serves as an interface between your secure web server and a VA. Together they validate certificates that have been issued by certification authorities (CAs) that the VA and the web server have been configured to recognize. Alternatively, the Web Server Validator can use certificate revocation lists (CRLs) provided by CAs for validating certificates.

The Web Server Validator for Microsoft IIS consists of the ISAPI filter (a dynamic link library, or DLL).

The ISAPI filter extracts the certificate information required for validation and obtains validation information from a VA.

Web Server Validator for Netscape

The ValiCert Web Server Validator is a plug-in that ensures that your Netscape Enterprise Server (NES) does not accept revoked certificates during secure web connections. The Validator serves as an interface between your secure web server and the VA, and validates certificates from CAs that have registered with the VA.

Browser Validator

The ValiCert Browser Validator is a module that enables your Internet Explorer browser to use a VA, or certificate revocation lists (CRLs) to validate the following:

- ❖ Server certificates in SSL connections
- ❖ Digitally signed files downloaded from the Internet

Digitally signed files use Microsoft Authenticode technology, which enables software publishers to digitally sign their files to ensure users that they can trust their downloaded files. The following types of files can be digitally signed:

- ❖ .exe
- ❖ .cab
- ❖ .ocx
- ❖ .dll
- ❖ .ctl

For more information on Microsoft Authenticode technology, visit:

<http://msdn.microsoft.com/workshop/c-frame.htm#/workshop/security>

CHAPTER 2

Getting Started

This section provides instructions on installing the ValiCert Validator Suite components. The system requirements and pre-installation tasks for each Validator vary slightly. Before you begin the installation process, be sure that the appropriate system requirements and pre-installation tasks are met:

E-Mail Validator Requirements

To install the ValiCert E-Mail Validator, you need:

- ❖ An x86-based computer running Windows 95, Windows 98, or Windows NT 4.0 (Server or Workstation)
- ❖ Service Pack 3, 5 or above if running on Windows NT

Before you install the E-Mail Validator, perform the following pre-installation task:

- ❖ Install a ValiCert VA server or register for the ValiCert Global VA Service.

If your system meets the system requirements and you have performed the pre-installation task, you can install the E-Mail Validator.

Address Book Validator Requirements

To install the ValiCert Address Book Validator, you need:

- ❖ An x86-based computer running Windows 95, Windows 98, or Windows NT 4.0 (Server or Workstation)
- ❖ Service Pack 3, 5 or above if running on Windows NT
- ❖ Compatible e-mail address book

Before you install the Address Book Validator, install a ValiCert VA server or register for the ValiCert Global VA Service.

If your system meets the system requirements and you have performed the pre-installation task, you can install the Address Book Validator.

Web Server Validator (Microsoft IIS) Requirements

You can install the Web Server Validator for the Microsoft IIS 4.0 or the Personal Web Server 4.0.

- ❖ To install the Web Server Validator for the Microsoft IIS 4.0, you need to have Windows NT 4.0 (Server).
- ❖ To install the Web Server Validator for the Personal Web Server 4.0, you need to have Windows NT 4.0 (Workstation).

Be sure that your system also meets the system requirements listed in Table 1

Table 1. System Requirements

Requirement	Minimum	Recommended
Hardware	Intel 166 MHz Pentium-based or compatible systems.	Intel 300MHz Pentium-II based or compatible systems
Memory	32 MB	64 MB
Disk Space	20 MB	20 MB
Operating Systems	For Personal Web Server: Windows NT Workstation 4.0 or later*	Not applicable
	For Microsoft IIS: Windows NT Server 4.0 or later *	

* You can use Service pack 3, 5 or later.

Before you install the Web Server Validator, perform the following pre-installation tasks:

- ❖ Be sure that your web server is running with Secure Sockets Layer (SSL) and is set up for client authentication.
- ❖ Install a ValiCert VA server or register for the ValiCert Global VA Service.

If your system meets the system requirements listed in Table 1 and you have performed all of the pre-installation tasks, you can install the Web Server Validator for the Microsoft IIS.

Web Server Validator (Netscape) Requirements

You can install the Web Server Validator for the Netscape Enterprise Server on a Windows NT or UNIX system.

- ❖ To install the Web Server Validator on a Windows NT system, you need to have Netscape Enterprise Server (versions 3.5, 3.6, 3.61, or 4.0) running on Windows NT 4.0.
- ❖ To install the Web Server Validator on a UNIX system, you need to have the Netscape Enterprise Server running on a SPARC-based workstation (Solaris 2.5.1 or 2.6).

Be sure that your system meets the system requirements listed in Table 2 for Windows NT systems or Table 3 for UNIX systems.

Table 2 lists the system requirements for installing the Web Server Validator for Netscape Enterprise Server on Windows NT.

Table 2. System Requirements for Windows NT

Requirement	Minimum	Recommended
Hardware	Intel Pentium-based or compatible systems	Intel Pentium-II based or compatible systems
Memory	32 MB	64 MB
Disk Space	20 MB	20 MB
Operating Systems	Windows NT Workstation 4.0* or Windows NT Server 4.0*	Not applicable

* You can use Service pack 3, 5 or later.

Table 3 lists the system requirements for installing the Web Server Validator on UNIX.

Table 3. System Requirements for UNIX

Requirement	Minimum	Recommended
Hardware	Sun SPARC-based workstation	SunUltra or compatible
Memory	32 MB	64 MB
Disk Space	20 MB	20 MB
Operating Systems	Solaris 2.5.1 or 2.6	Not applicable

Before you install the Web Server Validator, perform the following pre-installation tasks:

- ❖ Be sure that you have administrative privileges on the machine where you will install the Web Server Validator.
- ❖ Be sure that Netscape Enterprise Server is properly installed and running on your system.
- ❖ Be sure that your web server is running with Secure Sockets Layer (SSL) and is set up to require client certificates.
- ❖ Be sure that you have the necessary privileges to modify your existing Netscape Enterprise Server installation.
- ❖ Install a ValiCert VA server or register for the ValiCert Global VA Service.

If your system meets the system requirements listed in Table 2 (for Windows NT) or Table 3 (for UNIX) and you have performed all of the pre-installation tasks, you can install the Web Server Validator for the Netscape Enterprise Server.

Browser Validator Requirements

To install the ValiCert Browser Validator, you need:

- ❖ An x86-based computer running Windows 95, Windows 98, or Windows NT 4.0 (Server or Workstation)
- ❖ Service Pack 3, 5 or above if running on Windows NT
- ❖ Compatible e-mail address book

Before you install the Browser Validator, perform the following pre-installation task:

- ❖ You have installed a ValiCert VA server or registered for the ValiCert Global VA Service.

If your system meets the system requirements and you have performed the pre-installation task, you can install the Browser Validator.

Installing the Validator Suite on Windows NT

The Validator Suite Installation program allows you to install any combination of the ValiCert Validator Suite, which is made up of the following components:

- ❖ E-Mail Validator for Microsoft Outlook 97/98
- ❖ Address Book Validator
- ❖ Web Server Validator for Microsoft Internet Information Server (IIS)
- ❖ Web Server Validator for Netscape Enterprise Server (NES)
- ❖ Browser Validator for Microsoft Internet Explorer

You can install one or more of these Validators during the same installation session.



NOTE: If you have a Validator installed on your system, to upgrade that Validator, you must remove it and install the new version.

Be sure that the following applications are closed before you run the installation program.

If you are installing	Close
E-Mail Validator	Microsoft Outlook
Web Server Validator for Microsoft IIS	Microsoft Internet Explorer and Web Server IIS/PWS
Web Server Validator for Netscape Enterprise Server	Netscape Enterprise Server
Browser Validator	Microsoft Internet Explorer and Web Server IIS/PWS

To install the ValiCert Validator Suite on Windows NT

- Step 1 Insert the CD containing the ValiCert Validator Suite into your CD-ROM drive.
- Step 2 Double click on the self-extracting file Validator32Setup.
- Step 3 The Installation Folder dialog box displays.
Select a folder to extract the installation files into. If the folder does not exist you are prompted to create it.
- Step 4 Click **Finish**.
- Step 5 The installation files are unpacked and the Setup.exe program starts automatically. The InstallShield Wizard launches and the Welcome dialog box displays.
Follow the on-screen instructions as you proceed through the installation.
The **Next** button allows you to move forward to the next installation window.
The **Back** button allows you to go back to the previous installation window
The **Cancel** button closes the installation program without installing any component of the Validator suite. You will need to rerun the installation program again.
- Step 6 Click **Next**.
The ValiCert Software License Agreement dialog box displays.
- Step 7 Click **Yes** to accept the terms of the agreement.
The User Information dialog box displays.
- Step 8 Enter your user information.
You must provide your user name and company name. These are required fields.

Step 9 Click **Next**.

The Select VA Type screen displays:

Select VA Type

Select Configuration

☐ VA using File

☒ Manual

☐ GVAS

VA Host

Host Name Port No.

Proxy Server

☐ Proxy Server Used

Proxy Host Proxy Port

In the Select Configuration section, select the type of VA. The options are:

VA using file—Select this option for an Enterprise VA. When The Enterprise VA is installed a file is generated that contains the host, port and certificate of the VA.

Browse to locate the file, called `vaclient.dat` (the default location is `<VAInstallDir>\entserv\vaclient.dat`).

To use a proxy server, enter the **Proxy Host** and the **Proxy Port** in the Proxy Server section.

Manual—Select this option to manually enter the VA information. In the VA Host section, enter the **Host Name** and **Port No.** of the VA.

To use a proxy server, enter the **Proxy Host** and the **Proxy Port** in the Proxy Server section.

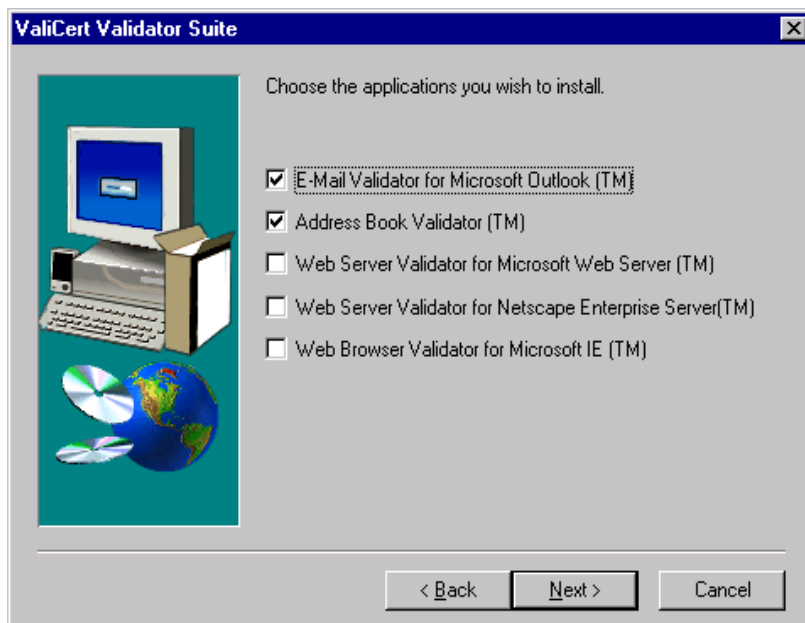
GVAS—Select this option to use the Global Validation Authority Service (GVAS).



NOTE: To use Global VA Service you need an account. See <http://www.ValiCert.com/html/gvas.html> for more information.

Step 10 Click **Next**.

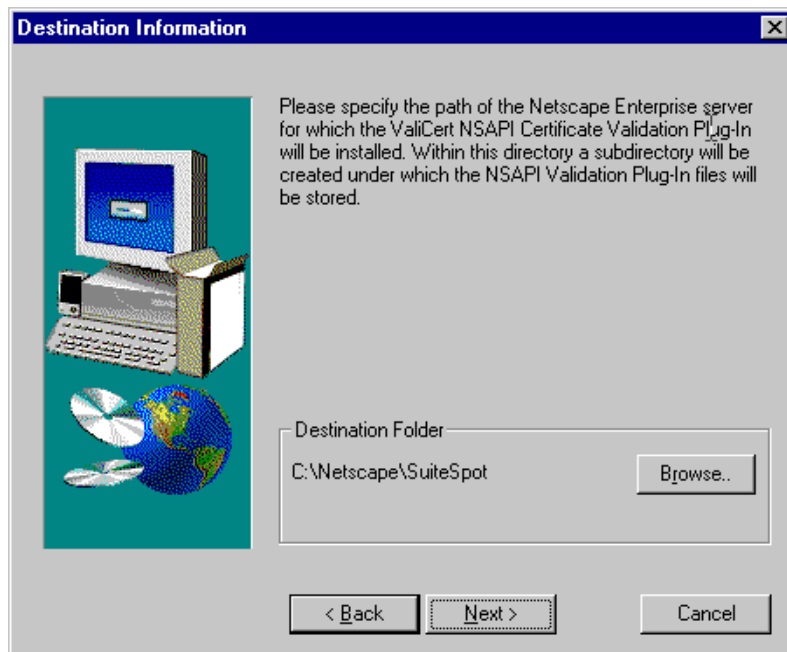
The ValiCert Validator Suite dialog box displays.



Step 11 Select one or more Validators to install. If you selected the Web Server Validator for Netscape Enterprise Server, continue with the next step, otherwise skip to Step 13.

Step 12 Click **Next**.

If you are installing the Web Server Validator for Netscape Enterprise Server, the Destination Information dialog box displays.

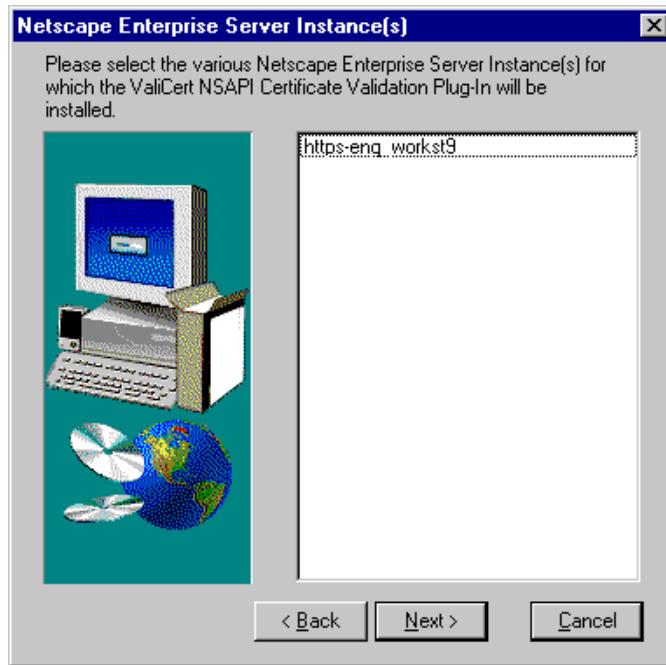


a Click **Browse** to choose a destination directory.

Choose the top-level directory of the Netscape Enterprise Server installed on your machine.

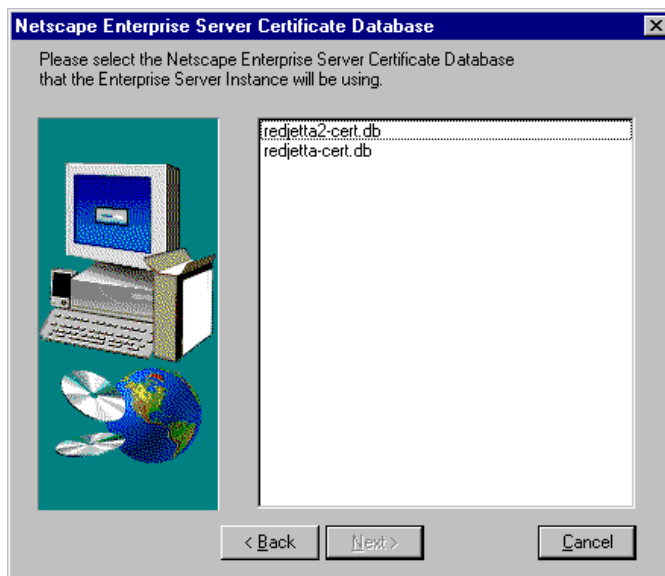
- b Click **Next**.

The Netscape Server Instance(s) dialog box displays.



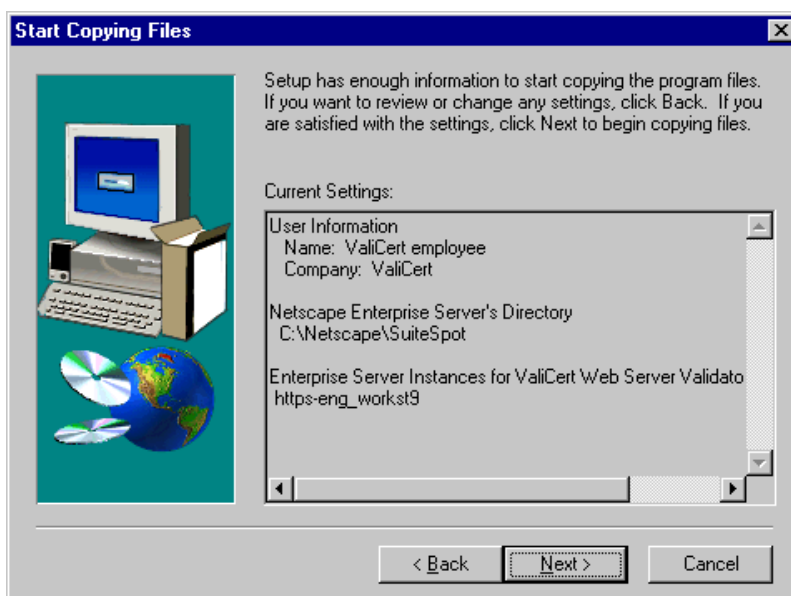
- c Select the server instance for which the Validator will be installed.
d Click **Next**.

- e The Netscape Enterprise Server Certificate Database dialog displays.



- f Select a certificate database from the list.
g Click **Next**.

The Start Copying Files dialog box for the Netscape Enterprise Server program files displays.



The install program is ready to copy program files for the Netscape Enterprise Server.

Skip to Step 15.

Step 13 Click **Next**.

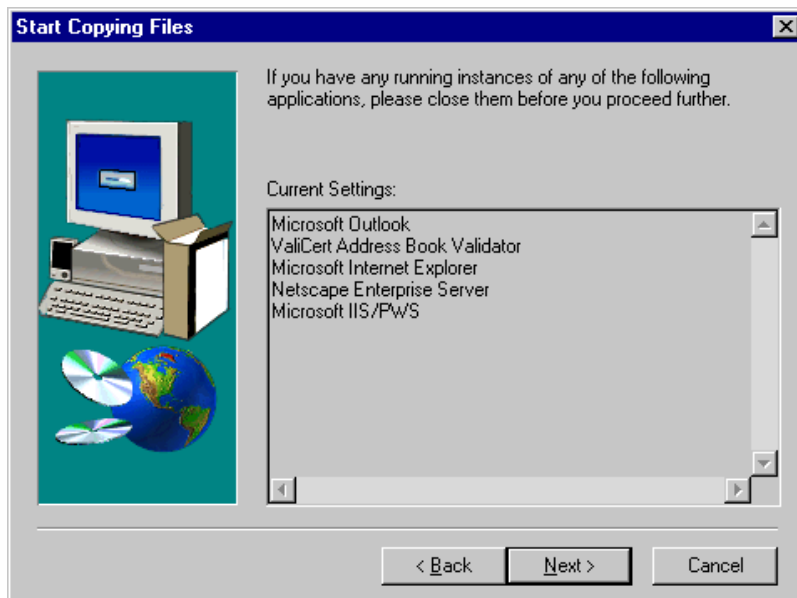
The Choose Destination Location dialog box displays.

Step 14 Choose a destination directory for the Validator Suite components.

Use the default directory or click **Browse** to choose another destination.

Step 15 Click **Next**.

The Start Copying Files dialog box displays:

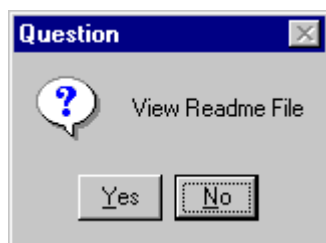


Step 16 Close any of the programs listed in the dialog box.

Step 17 Click **Next**.

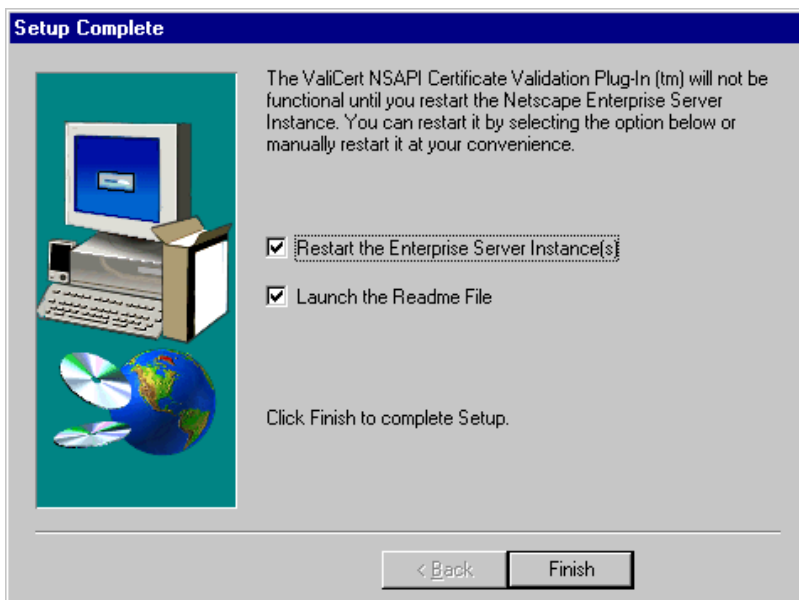
Files for the Validator Suite components are copied from the installation directory to the specified destination directory.

If you selected a Validator other than the Web Server Validator for the Netscape Enterprise Server to be installed, the Question Dialog box displays:



- a Click **Yes** to read the latest ValiCert Suite information now or **No** to continue with installation without reading the Readme file. The Setup program exits.

If you selected the Web Server Validator for the Netscape Enterprise Server to be installed (by itself or with any of the other Validators) files are copied to the specified destination directory, and the Setup Complete dialog box displays:



- b Select the appropriate options.

To restart the server select **Restart the Enterprise Server Instances**. The setup program stops and restarts the instance of the Netscape Enterprise Server.

Select **Launch the Readme File**, to view the current Readme file for the Validator Suite.

- c Click **Finish**.

The installation program closes.

The ValiCert Validator Suite is added to your Start menu. From the ValiCert Validator program option, you can view the Readme file for the latest ValiCert Validator Suite information or start any of the installed ValiCert Validator applications. You are now ready to configure and use the installed Validators.

If you have installed the Web Server Validator for Netscape Enterprise Server, proceed with "Modifications to obj.conf File for the Web Server Validator for Netscape."

Modifications to obj.conf File for the Web Server Validator for Netscape

The Web Server Validator for the Netscape Enterprise Server installation program adds the following lines to your server's `obj.conf` file:

```
Init fn="load-modules" funcs="init_fn,test_auth" shlib=<PathToModule>  
Init fn="init_fn" vc-config-file=<PathToConfigFile>
```

It also adds the following lines inside the default object in the `obj.conf` file:

```
PathCheck fn="test_auth"
```

You can now configure and use the Web Server Validator for the Netscape Enterprise Server. Proceed to Chapter 7, "Using Validator for Netscape Server."

Installing the Web Server Validator for Netscape on UNIX

This section describes how to install the Web Server Validator for Netscape Enterprise Server on a UNIX platform. It assumes that your system meets the system requirements described in "Web Server Validator (Netscape) Requirements" on page 7.

You install the ValiCert Web Server Validator for Netscape Enterprise Server in much the same way you install other Solaris software packages. For information on packages, refer to the `pkgadd`, `pkginfo`, and `pkgrm` man pages.



NOTE: To add a package, you need to log in as "root" on the system where you are installing the package.

To install on the UNIX platform

- Step 1 Extract the ValiCert Web Server Validator for Netscape Enterprise Server package from the tar archive by entering the following from the directory where you downloaded the `VCVal.tar` file.

```
tar -xvf ./VCVal.tar
```

- Step 2 Log on as "root" on the machine where you want to install the Web Server Validator.

- Step 3 Open a shell window and enter the following at the command prompt:

```
pkgadd -d .
```

The **pkgadd** menu displays.

- Step 4 Select **VCRTnsapi** as the package you want to install, then follow the on-screen instructions.

The installation program prompts you for the server location, installs the files, and edits your `obj.conf` file and `vcnsapi.ini` file.

The installation program adds the following lines to your server's `obj.conf` file:

```
Init fn=load-modules shlib=<ModulePath>funcs="init_fn,test_auth"  
Init fn=init_fn vc-config-file= <PathToConfigFile>
```

It also adds the following lines inside the default object in the `obj.conf` file:

```
PathCheck fn="test_auth"  
NameTrans fn="pfx2dir" from="/valicert" dir="<doc-root>/valicert"
```

You can now configure and use the Web Server Validator for Netscape Enterprise Server. Proceed to Chapter 7, "Using Validator for Netscape Server."

Configuring the E-Mail Validator

This section describes how to configure the ValiCert E-Mail Validator after you have installed it. The ValiCert E-Mail Validator is a Microsoft Outlook Add-In module that lets you check the status of digital certificates used to sign S/MIME email. You can also use the module to send Freshness Proof stamps (certificate validation proof) with a signed e-mail.

You need to specify how certificates are validated at your site and how the Validator will handle Freshness Proof stamps for delivering and receiving messages. Your system administrator should provide you with this information.

Configuring the E-Mail Validator

Configure the Validator through the Certificate Validation Options dialog box. The configurations options is added to the Tools menu in Outlook when the Validator is installed.

To configure the E-Mail Validator

- Step 1 Select **Certificate Validation Options** from the Microsoft Outlook **Tools** menu.

The following dialog box displays:



Step 2 Configure the Validator as instructed by your site administrator.

The available options are as follows:

In the **Validate Certificate using** section, select the type of VA that will be contacted for validation. Choose one of the following options:

ValiCert Global VA Service – The E-Mail Validator will contact the ValiCert Global VA Service directly to validate certificates.

ValiCert Enterprise VA – The E-Mail Validator will contact the specified ValiCert Enterprise VA or ValiCert Certificate VA to validate certificates.

By default, the host name and the port number for the VA, which were specified during installation, are used.

Local Data Store – The Validator will use locally stored certificate revocation lists (CRLs) to validate certificates.

In the **Validation Protocol & Certificate Stores** section, select the protocol that the Validator will use for validation and indicate the

certificate store for trusted certificates. Your options depend on the selection you made from the **Validate Certificate using** section.

CRT – Certificate Revocation Tree™ protocol. Specify the path to the validation server certificate if you select this option.

OCSP – Online Certificate Status Protocol. Specify the path to the validation server certificate if you select this option.

CRL– Certificate Revocation List. Specify the path to the `vcCRL.ini` file which contains entries which point to CRLs.

In the **ValiCert Freshness Proof Stamp** section, select the options you want to enable. These options are only available with the CRT protocol. The available options are as follows:

Add Freshness Proof Stamp to Outgoing Messages – Select this option to include the Freshness Proof stamp with your outgoing messages. When this option is enabled, the Validator validates your signing certificate whenever you send a signed message and attach a Freshness Proof stamp to the message. The Freshness Proof stamp assures the recipients of your signed message that your certificate was valid at the time the message was signed and sent. If the recipients trust the Freshness Proof stamp they will not check the validation status of your message.

Trust Freshness Proof Stamp of Incoming Messages – When this option is enabled, the Validator will not check the revocation status of messages that include a Freshness Proof stamp, because it is assumed that the certificates used to sign such messages are valid. If this option is not enabled, the Validator checks the revocation status of every received message, regardless of whether or not a Freshness Proof stamp has been attached to it.



NOTE: If the Freshness Proof stamp for the E-Mail Validator has expired, and the end user is trusting the Freshness Proof stamp, the user is not notified of the expired Freshness Proof stamp.

Step 3 Click **OK** to apply the settings you just selected.

Creating the CRL Initialization File

If you are using CRLs to validate certificates, you might need to create or edit an initialization file (named `vcCRL.ini`) that contains information about the CAs that issue the CRLs. Your site administrator may have provided you with such a file.

To create or edit the file, use the following format for each CA that issues CRLs.

```
VC_CA_<ca_number>_PUB_KEY_HASH=<hash>
VC_CA_<ca_number>_CRL_TYPE=<crl_type>
VC_CA_<ca_number>_CRL_URL=<crl_url>
```

The following table lists and briefly describes each of the variables:

Variable	Description
<code>ca_number</code>	Number of the entry in the file. For example, 1 for the first CA listed, 2 for the second, and so forth.
<code>hash</code>	Public key hash of the CA certificate. You can get this from your site administrator or by using the <code>dumppubkeyhash.exe</code> program (located in the Validator Suite directory by default).
<code>crl_type</code>	CRL Type. The value 0 specifies DER-encoded (binary) CRLs and 1 specifies base-64-encoded (ASCII) CRLs.
<code>crl_url</code>	LDAP or HTTP URL of the CRL.

The following is an example of an entry:

```
VC_CA_1_PUB_KEY_HASH=082917F8CFE82DFCEBE23B94769377285E9F81DE
VC_CA_1_CRL_TYPE=0
VC_CA_1_CRL_URL=http://bravo/CertSrv/bravo.crl
```

Adding Trusted Root Certificates

To verify the status of a digital certificate used to sign an email, the Validator must trust the certificate. A certificate is trusted if the Certification Authority (CA) that signs the certificate is known to the Validator. In order to trust a CA, the Root certificate of the CA must be stored in your Windows certificate store.

You must install the Root certificates of any CAs that will sign certificates of mail you receive. Your site administrator will tell you which certificates you need to obtain and where to get them.

Most public CAs root certificates come bundled with Outlook. Usually you will only need to add Root certificates of Enterprise CAs (CAs local to your installation). In this case the Root certificate will likely be available on a local certificate server, like the Microsoft Certificate Server. For the purpose of illustration, instructions on adding a certificate from a Microsoft Certificate Server are provided. For more instructions on adding certificates see “Adding Trusted Root Certificates” on page 53.



NOTE: You will need Internet Explorer 4.01 or later to add certificates, but version 5.0 or later is recommended.

To add a new local Microsoft Certificate Server's certificate to your certificate database

Step 1 Go to the URL of the site containing a hyperlink to the actual certificate.

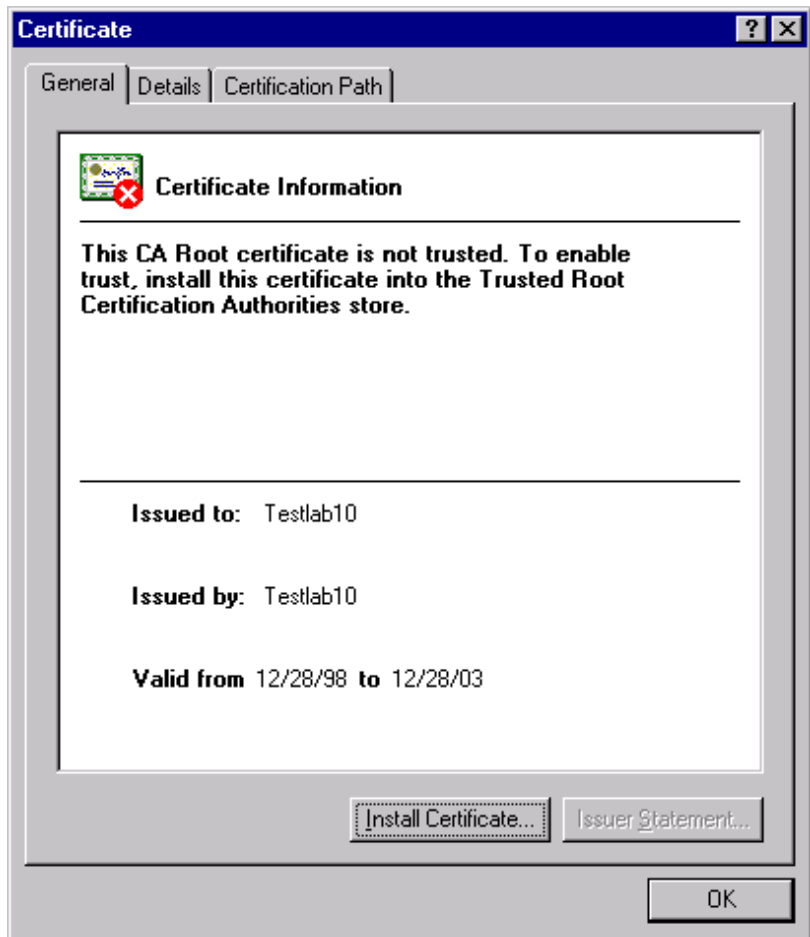
For example, if you are obtaining a certificate from a Microsoft Certificate Server, you will see a page similar to the following.



Step 2 Click on the link to the certificate.

A dialog box displays asking if you want to open the file or save it to disk.

- Step 3 Select the open the file option and click **OK**.
The Certificate dialog displays.

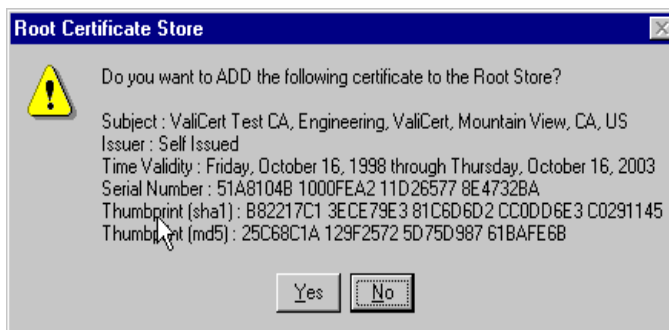


Step 4 Click **Install Certificate.**

The Certificate Manager Import Wizard launches.

Follow the instructions to import the certificate into the Windows certificate store.

In the last step, the following dialog displays to confirm that you want to add the certificate.



Step 5 Click **Yes to add the certificate to your Windows certificate database.**

The certificate is added to your database.

Viewing CA Certificates

You can verify that you have added the CA certificate. In addition you can view other certificates in your certificate database.



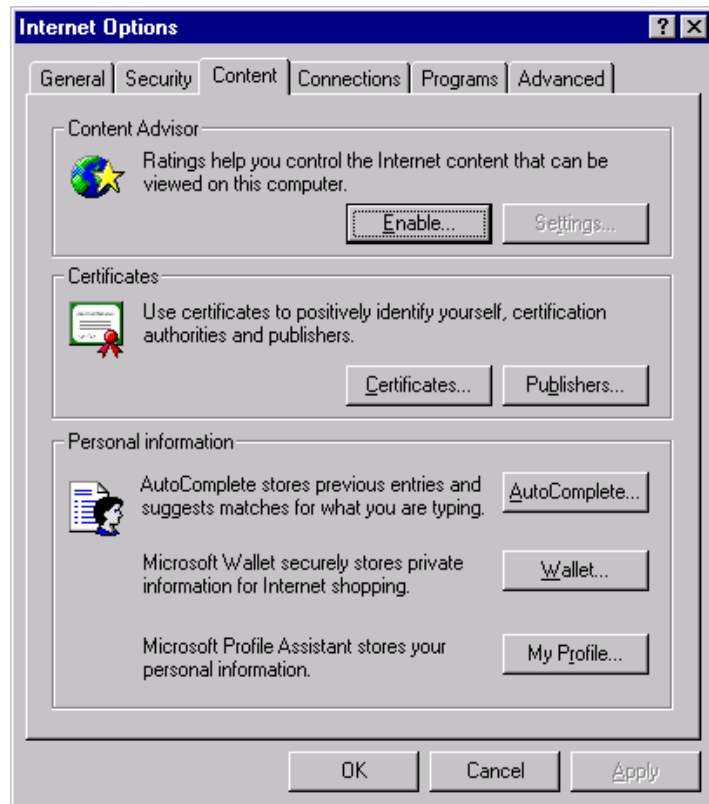
NOTE: These instructions are for using Internet Explorer 5.0. For other versions or browsers, consult the user documentation.

To view CA certificates

Step 1 Open the **Internet Options** control panel (**Tools > Internet Options**).

Step 1 Click the **Content** tab.

The following dialog box displays.

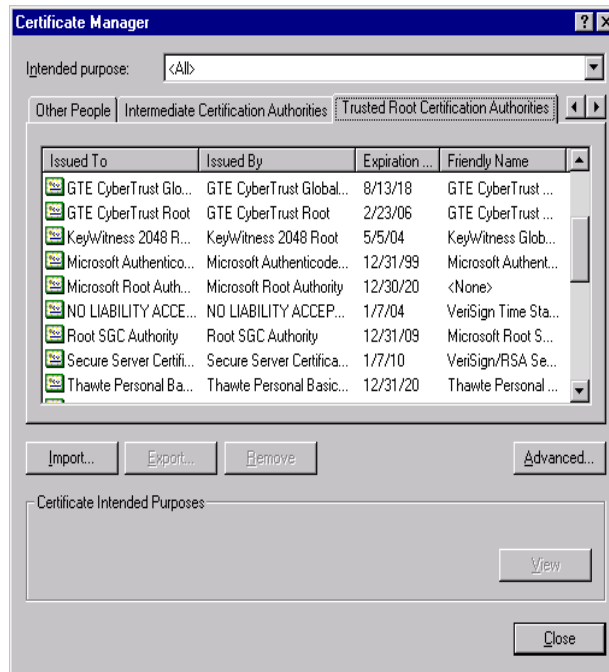


Step 2 Click **Certificates**.

The Certificate Manager displays.

Click the **Trusted Root Certification Authorities** tab.

The following dialog box displays:



Step 3 Scroll through the list of trusted CAs to locate the newly added certificate.

Using the E-Mail Validator

This section describes how to start and stop the add-in, and how to use the e-mail add-in features when sending, reading, and receiving e-mail messages with Microsoft Outlook.

Starting and Stopping the E-Mail Validator

Similar to other Microsoft Outlook add-ins, use the Outlook Add-In Manager to start and stop the E-Mail Validator. By default, the E-Mail Validator is enabled upon installation. You can tell if the Validator is running if the **ValiCert E-Mail Validator** box is checked in the Add-In Manager.

To use the Add-In Manager to start and stop the Validator:

- Step 1 Select **Options** from the Microsoft Outlook **Tools** menu.
- Step 2 Click the **Other** tab.
- Step 3 Click **Advanced Options**.
- Step 4 Click **Add-In Manager**.
- Step 5 To stop the Validator, make sure that the **ValiCert E-Mail Validator** box is not selected. To start the Validator, make sure that the **ValiCert E-Mail Validator** box is selected.
You can toggle this selection to start and stop the Validator.

Sending Signed E-Mail Messages

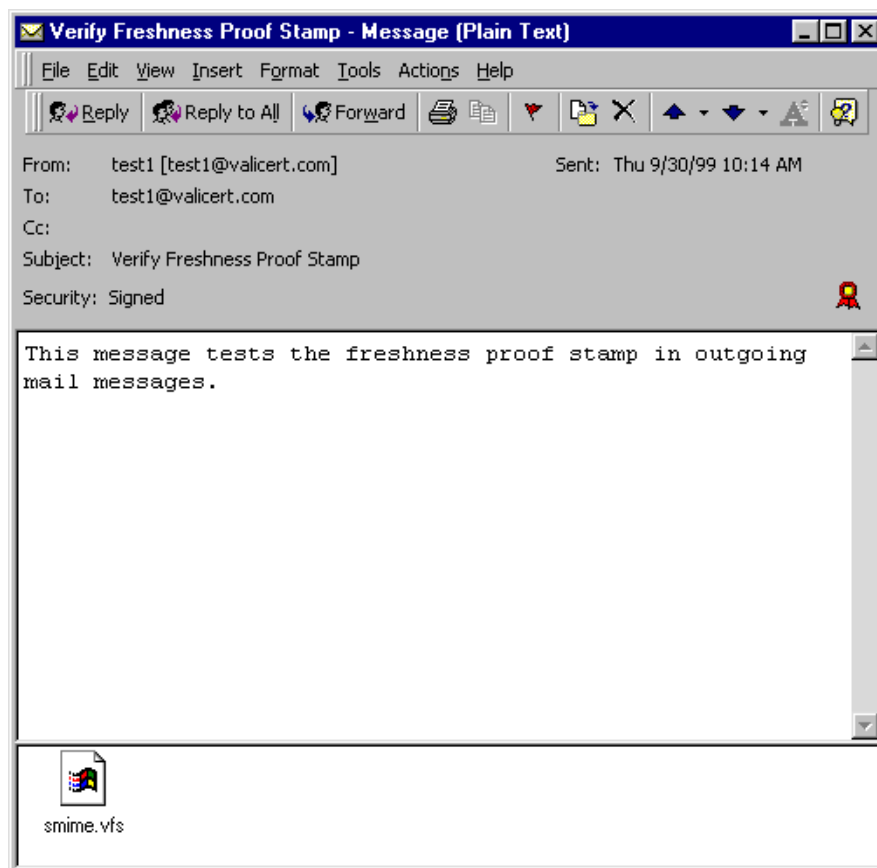
If you have selected **Add Freshness Proof Stamp to Outgoing Messages** in **Certificate Validation Options** a Freshness Proof stamp will be added to every outgoing message you send. The Freshness Proof stamp is a MIME

attachment that tells the recipients of your message that you have validated the certificate used to sign the message. As a result, recipients of your message do not have to validate the certificate.



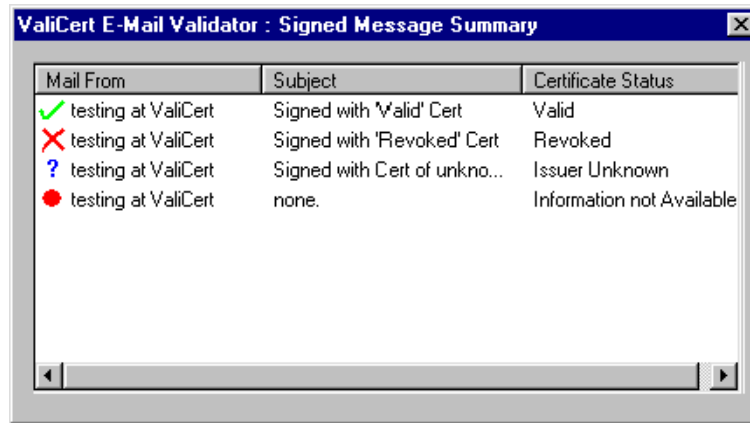
NOTE: This is especially useful when sending a message to a large number of users: instead of having each recipient obtain validation information for your certificate, you only need to obtain the information once and the recipients will be able to trust your message just as if they used the server.

You can verify that a Freshness Proof stamp has been added to a message by opening the message in your outbox. If a Freshness Proof stamp had been attached, you will see an `smime.vfs` attachment, as in the following diagram.







Receiving E-Mail

When you receive signed e-mail messages, the Validator automatically checks whether or not the certificate(s) used to sign the message(s) have been revoked, and displays the following dialog box.



The icons (described in Table 4), appear on the left-hand column of the dialog, and represent the status of each received signed message.

Table 4. Message Status Icons

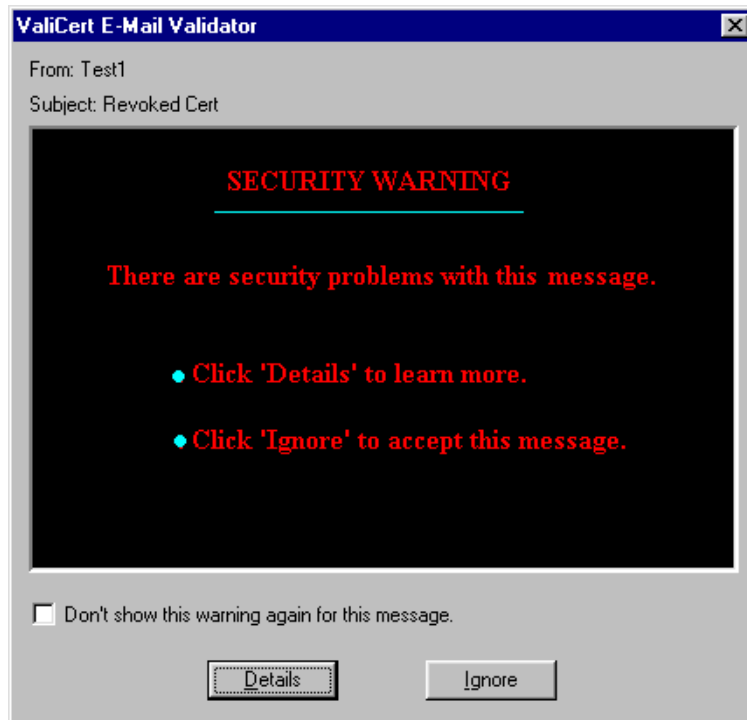
	The message was signed by a valid certificate.
	The message was signed by a revoked certificate.
	The message was signed by a certificate whose issuer is unknown.
	The message was signed by a certificate that could not be validated. Read the following section for information on why a certificate might not be validated.

Reading E-Mail

This section describes how the ValiCert E-Mail Validator works when you use Microsoft Outlook to read signed e-mail messages. The Validator stores the validation status of the e-mail message in the MAPI store of Outlook 98 or Outlook 2000. When you read a signed message, the Validator retrieves the validation status from the e-mail message and displays information as described below.

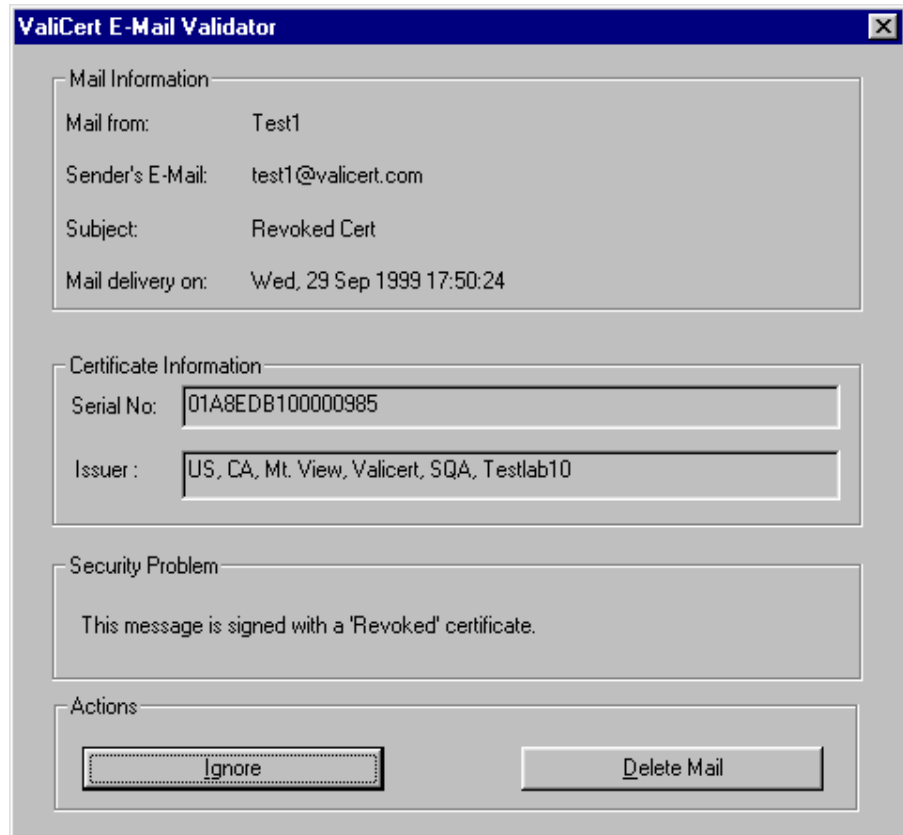
Revoked Certificates

If you open a message that has been signed by a revoked certificate, the following dialog box appears:



You can choose to view the revocation information, or you can ignore the message. In addition, you can select the **Don't show this warning again for this message** check box, to prevent this dialog from being displayed when you open the message again.

If you choose to ignore the warning, you can read the message just as you normally would. If you view the revocation information, a dialog box similar to the following appears:

A screenshot of a Windows-style dialog box titled "ValiCert E-Mail Validator". The dialog box has a blue title bar with a close button in the top right corner. It contains four sections: "Mail Information" with fields for "Mail from: Test1", "Sender's E-Mail: test1@valicert.com", "Subject: Revoked Cert", and "Mail delivery on: Wed, 29 Sep 1999 17:50:24"; "Certificate Information" with "Serial No: 01A8EDB100000985" and "Issuer: US, CA, Mt. View, Valicert, SQA, Testlab10"; "Security Problem" with the text "This message is signed with a 'Revoked' certificate."; and "Actions" with two buttons: "Ignore" and "Delete Mail".

Mail Information	
Mail from:	Test1
Sender's E-Mail:	test1@valicert.com
Subject:	Revoked Cert
Mail delivery on:	Wed, 29 Sep 1999 17:50:24

Certificate Information	
Serial No:	01A8EDB100000985
Issuer :	US, CA, Mt. View, Valicert, SQA, Testlab10

Security Problem
This message is signed with a 'Revoked' certificate.

Actions
<input type="button" value="Ignore"/> <input type="button" value="Delete Mail"/>

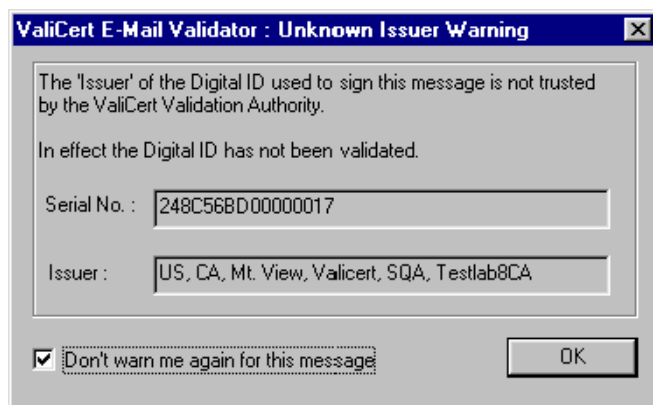
After you have reviewed the information, click **Ignore** to proceed with reading the message or you click **Delete Mail** to delete the mail and send it to your **Deleted Items** folder.



NOTE: You will have to delete messages from the **Deleted Items** folder manually.

Unknown Issuers

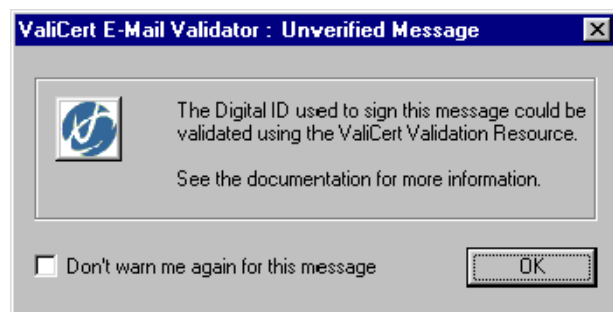
If you open an e-mail message signed by a certificate from a CA not recognized by the validation server, the following dialog appears:



If the CA is one that should be trusted, consult your site administrator for information on how to add the root certificate for this CA to your list of trusted issuers.

Certificates with Unknown Status

If you open an e-mail message whose certificate could not be verified, the following dialog appears:



NOTE: Be sure to restart the Outlook if you make any of the configuration changes described below.

If using the ValiCert Global VA Service, ValiCert Enterprise VA, or ValiCert Certificate VA for validation, the unverified message can appear for any of the following reasons:

- ❖ The ValiCert Enterprise VA or ValiCert Certificate VA may not be configured properly.

Confirm with your site administrator that the ValiCert Enterprise VA or ValiCert Certificate VA host name and port number are specified correctly in the Preferences dialog.

- ❖ The certificate for the ValiCert Enterprise VA or ValiCert Certificate VA may be corrupted, missing, or you may have incorrectly specified its location.

Make sure that the ValiCert Enterprise VA or ValiCert Certificate VA Base 64 (ASCII) certificate (typically named `ves.cert`) exists in the location specified in the CRT or OCSP (whichever is appropriate) box in the Preferences dialog. If the certificate is not in the location specified in the **CRT** or **OCSP** check box, change the specified location.

If the file is corrupted or missing, do the following.

- a Open the ValiCert Enterprise VA or ValiCert Certificate VA administration server in a web browser.
 - b Select **Manage Keys and Certificates** in the left pane of the window.
 - c Select **View VA Certificates**.
 - d Copy the base-64 encoded format of the certificate (at the bottom of the page) to the clipboard. Be sure to include the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines.
 - e Paste the contents of the clipboard in a text editor. Make sure that the `END CERTIFICATE` line appears on its own line.
 - f Save the file to any location.
 - g Use the **Browse** button in OCSP or CRT sections of the **Validation Protocol and Certificate Stores** section of the Certificate Validation Options dialog to specify the location of this file.
- ❖ The CA that issued the certificate may not be in your list of trusted issuers.

Ensure that it is. If not, see “Adding Trusted Root Certificates” on page 25 for information on how to add the CA root certificate to your list of trusted issuers.

- ❖ You may be experiencing network problems.

Use a web browser to connect to the ValiCert Enterprise VA or ValiCert Certificate VA.

If using a local data store for validation, the unverified message can appear for any of the following reasons:

- ❖ The CRL initialization file may be missing, corrupted, or expired.
Ensure that the file (typically named `vcCRL.ini`) is present and its location is specified correctly in the **CRL** path field in the Certificate Validation Options dialog box.
- ❖ The initialization file might not contain an entry for the CA who has issued the certificate you want to validate (See “Creating the CRL Initialization File” on page 24).

CHAPTER 5

Using the Address Book Validator

This section describes how to use the ValiCert Address Book Validator. It includes information about:


- ❖ Starting the Address Book Validator
- ❖ Stopping the Address Book Validator
- ❖ Opening the Main Dialog box
- ❖ Configuring the Address Book Validator
- ❖ Validating Certificates
- ❖ Viewing Certificate Status
- ❖ Adding Trusted Root Certificates
- ❖ Sharing Contacts Address Book
- ❖ Creating the CRL Initialization File

Starting the Address Book Validator

To start the ValiCert Address Book Validator

Step 1 At the **Start** menu, choose **Address Book Validator** from the **Programs > ValiCert Validator Suite** drop-down list.

The ValiCert splash screen displays briefly.

When the Address Book Validator starts, the  icon displays in your system tray indicating you are now ready to use the Address Book Validator. The system tray typically displays in the lower right portion of the Start Toolbar.

For instructions on configuring the Validator see “Configuring the Address Book Validator” on page 41.

Stopping the Address Book Validator

You can stop the Address Book Validator at anytime.

To stop the ValiCert Address Book Validator

Step 1 Right-click the  icon in the system tray.

Step 2 Click **Exit** from the pop-up menu.

The icon disappears from the system tray, indicating that the application is no longer running.

Opening the Main Dialog box

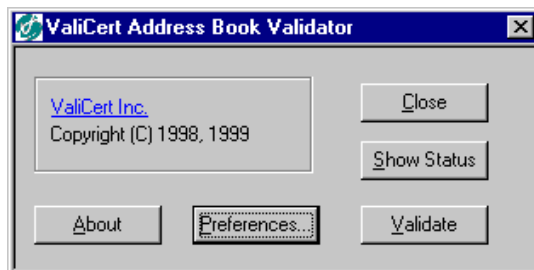
The Address Book Validator provides a dialog box that contains all of the options available to you when using the Address Book Validator.

To open the main dialog box

Step 1 Right-click the  icon in the system tray.

Step 2 Select Open from the pop-up menu.

The main ValiCert Address Book Validator dialog box displays.



Step 3 Click the option that you want.

Click **About**, **Preferences**, or **Show Status** to access the corresponding dialog box.

Click **Validate** to validate the certificates currently in the Windows Address Book database.

Click **Close** to close this dialog box.

Configuring the Address Book Validator

To configure the Address Book Validator to suit your needs use the Preferences dialog. You must configure the Address Book Validator the first time you run it. The configuration information is stored for use in subsequent sessions.

Configuring the Address Book Validator involves the following tasks.

- ❖ Opening the Preferences Dialog Box
- ❖ Configuring the Activity Log
- ❖ Configuring Alert Settings
- ❖ Configuring Connection Settings to Proxy Server
- ❖ Configuring Your Address Books
- ❖ Configuring Validation Settings



NOTE: With the exception of opening the Preferences dialog box, you can perform these tasks in any order.

When you have configured your preferences, click **Apply** or **OK** to apply the changes.


- ❖ Click **Apply** to apply your changes without closing the Preferences dialog box.
- ❖ Click **OK** to apply your changes and to close the Preferences dialog box.



NOTE: Applying your changes updates the hard disk and registry with the preferences you have configured,

Opening the Preferences Dialog Box

To open the Preferences dialog box

- Step 1 Right-click the  icon in the system tray.
- Step 2 Select **Preferences** from the pop-up menu.
- The ValiCert Address Book Validator Preferences dialog box displays with the Activity log tab active.
- Configure your preferences at the various tabs. The tabs in the ValiCert Address Book Validator Preferences dialog are described in the following sections.



NOTE: You can also open the Preferences dialog box from the main dialog box by clicking **Preferences**. See “Opening the Main Dialog box” on page 40.

Configuring the Activity Log

The Address Book Validator creates and constantly updates an activity log with events that you want monitored and logged when encountered by the Address Book Validator.

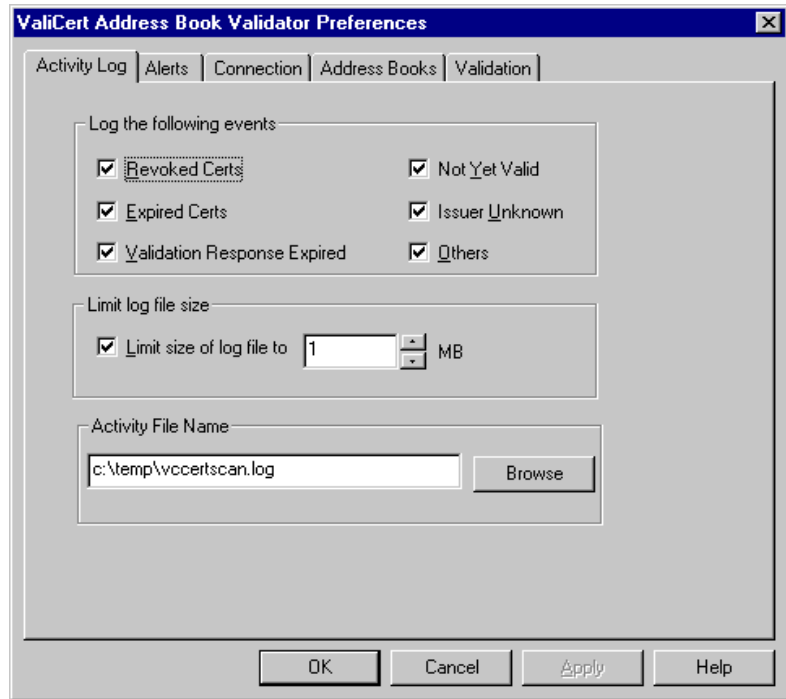
To configure the Activity log

- Step 1 Select the Activity Log tab from the ValiCert Address Book Validator Preferences dialog box.



NOTE: When you first open the Preferences dialog box, the Activity Log tab is selected and displays.

The Activity Log tab displays:



Step 2 Select the events you want monitored and logged in the activity log when encountered by the Address Book Validator.

Select from the following events:

Revoked Certs—Any certificate that has been revoked by the issuer of the certificate. A revoked certificate can be in a CRL or CRT.

Expired Certs—Any certificates that have expired. Every X.509 certificate has a validity period field that defines a time interval (start date and end date) during which the CA must maintain information about a certificate's status. Once the end date elapses, the certificate expires.

Validation Response Expired—Any certificate revocation lists and certificate revocation trees that have expired. The expiration of a CRL and CRT is determined by the value of the `nextUpdate` parameter in the CRL or CRT.

Not Yet Valid—Any certificate that is in the database, but has a validity period in the future.

Issuer Unknown—Any certificate for which the issuer of the certificate is not known to the Address Book Validator. This means that the issuer is not contained in the server's certificate database.

Others—Any certificate not within the other categories. For example, if the Address Book Validator is unable to communicate with the VA.

Step 3 Set the maximum size of the activity log.

When the activity log reaches the specified size (in megabytes), the Address Book Validator creates a new file with the current date and time as its extension, (for example, *logfile.timestamp.format*).



NOTE: We recommend that you keep the latest log file, and delete the older versions.

Step 4 Specify the path and the name of the activity log file.

By default, the activity log is named `c:\temp\vccertscan.log`.

Step 5 Click **Apply** to apply your changes now or skip to the next step.

Step 6 Click another tab to continue configuring preferences or click **OK** to exit the Preferences dialog box.

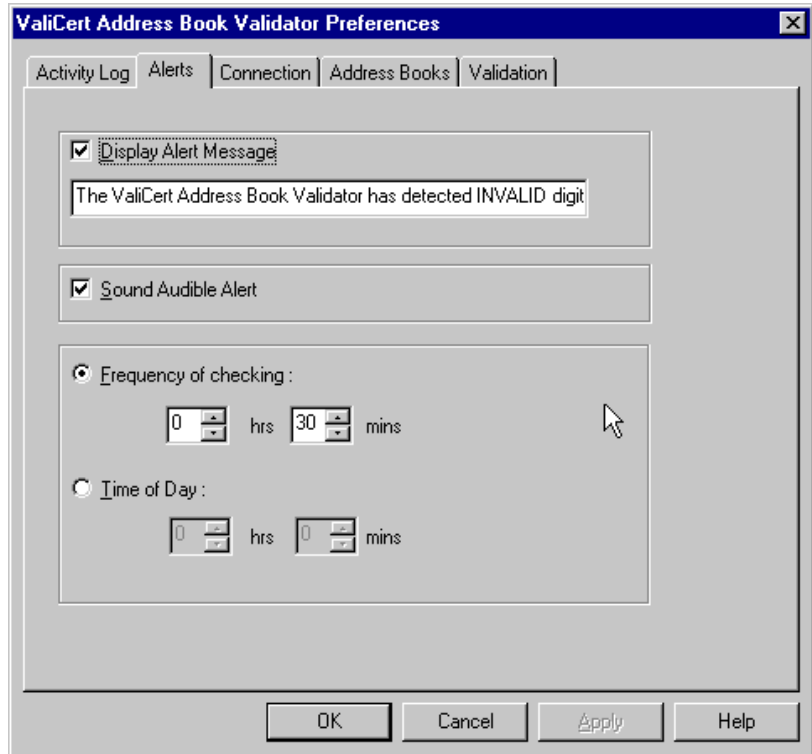
Configuring Alert Settings

The ValiCert Address Book Validator can give visual and audio alerts when it encounters invalid certificates in your Address Book. You can configure these In addition, you can specify when, or how frequently the application checks your Address Book.

To configure the Alerts

Step 1 Select the Alerts tab from the ValiCert Address Book Validator Preferences dialog box.

The Alerts tab displays:



Step 2 Select any alert types you want when the Address Book Validator encounters an invalid certificate.

Select from the following alert types:

Display Alert Message—Displays an alert message whenever the Address Book Validator encounters an invalid certificate. You can also specify the message that displays, up to 128 characters in length.

Sound Audible Alert—Provides an audible sound whenever the Address Book Validator encounters an invalid certificate.

- Step 3 Select the frequency at which the Address Book Validator checks for invalid certificates.

Select only one of the following types of interval:

Frequency of Checking—Checks the database for invalid certificates at the specified fixed interval. Select this radio button and specify how often you want the Address Book Validator to check certificates.

Time of Day—Checks the database for invalid certificates every day at the specified time. Select this radio button and specify the time when you want the Address Book Validator to check certificates.

- Step 4 Click **Apply** to apply your changes now or skip to the next step.

- Step 5 Click another tab to continue configuring preferences or click **OK** to exit the Preferences dialog box.

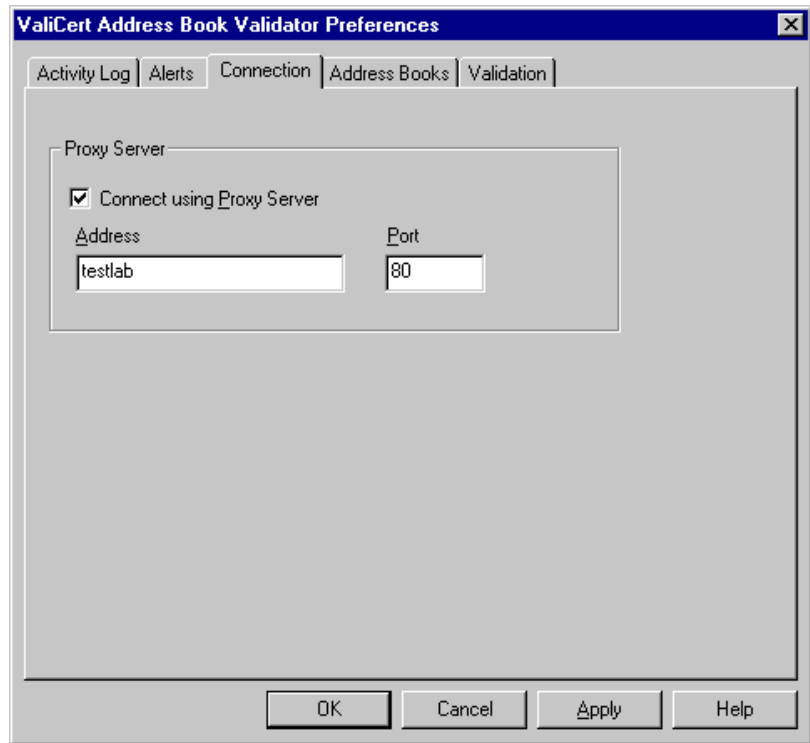
Configuring Connection Settings to Proxy Server

You may need to configure the Address Book Validator to communicate with your validation server via a proxy server. You will need a proxy server if you wish to communicate to a validation server that is located outside your local network (for example, ValiCert's Global Validation Authority Service) and your firewall prohibits direct connections to the specified server.

To configure connection settings

- Step 1 Select the Connection tab from the ValiCert Address Book Validator Preferences dialog box.

The Connection tab displays:



Step 2 Check the **Select the Connect using Proxy Server** box.

Step 3 Enter the proxy server's fully qualified network name or IP address and port number in the appropriate fields.

The following is an example of the information you need to enter in these fields:

```
tester1.valicert.com  
80
```

Step 4 Click **Apply** to apply your changes now or skip to the next step.

Step 5 Click another tab to continue configuring preferences or click **OK** to exit the Preferences dialog box.

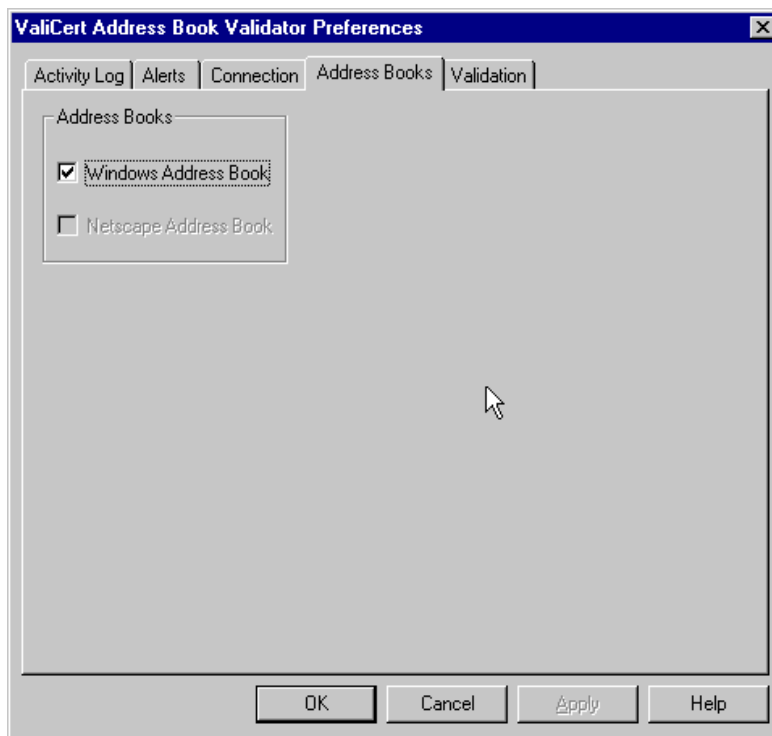
Configuring Your Address Books

The ValiCert Address Book Validator currently supports the Microsoft Windows Address Book.

To configure your address books

Step 1 Select the Address Books tab from the ValiCert Address Book Validator Preferences dialog box.

The Address Books tab displays:



Step 2 Check the **Windows Address Book** box.

This option is selected by default.

Step 3 Click **Apply** to apply your changes now or skip to the next step.

Step 4 Click another tab to continue configuring preferences or click **OK** to exit the Preferences dialog box.

Configuring Validation Settings

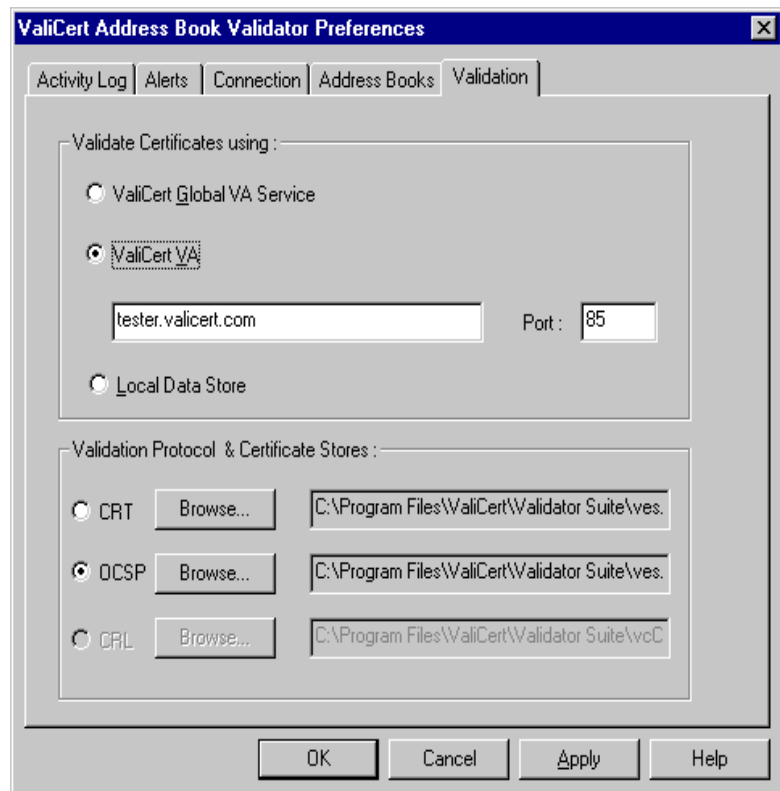
The Address Book Validator obtains certificate validation information from the ValiCert Global VA ServiceSM, ValiCert Enterprise VATM, or a local data store. By default, the Address Book Validator uses the method specified during installation.

If you are using the ValiCert Global VA Service or ValiCert Enterprise VA for validation, the supported protocols are CRT or OCSP. If you are using a local data store for validation, only CRLs are used.

To configure validation

- Step 1 Select the Validation tab from the ValiCert Address Book Validator Preferences dialog box.

The Validation tab displays:




- Step 2 Select the validation method the Address Book Validator uses to validate certificates.
If the application obtains validation information from a ValiCert Enterprise VA, indicate the name and port number of this server.
- Step 3 Specify the protocol you are using to communicate with the VA and the certificate stores you are accessing.
If you are using the ValiCert Global VA Service or ValiCert Enterprise VA for validation, specify the protocol you are using (CRT or OCSP) and the location of the certificate data store, which contains the certificate for the validation server.
If you are using a local data store for validation, specify the location of the `vcCRL.ini` file. This file contains information about the CRL(s) used to obtain validation information. For information on creating this file, see “Creating the CRL Initialization File” on page 58.
- Step 4 Click **Apply** to apply your changes now or skip to the next step.
- Step 5 Click another tab to continue configuring preferences or click **OK** to exit the Preferences dialog box.

Validating Certificates

You can validate the certificates in your Address Book at any time in addition to any time or interval you set in the Alert preferences. For information about configuring a specific validation time, see “Configuring Alert Settings” on page 44.

To validate certificates

- Step 1 Right-click the  icon in the system tray.
- Step 2 Select **Validate Now** from the pop-up menu.
The Validator checks the certificates in your Address Book.
An animated check mark displays on the icon, indicates that all the certificates in your Address Book are valid.
An X indicates that one or more certificates ion your Address Book are invalid.




NOTE: You can also validate certificates from the main dialog box by clicking **Validate**. See “Opening the Main Dialog box” on page 40.

Viewing Certificate Status

You can view the status of the certificates in your Address Book application at any time.

To view certificate status

- Step 1 Right-click the  icon in the system tray.
- Step 2 Select **Show Status** from the pop-up menu.

The Validation Status dialog box displays:

Validation Status as of Wednesday, March 22, 2000, 05:32 PM

No. of Entries : No. of Certificates :

No. of valid Certificates : No. of INVALID Certificates :

INVALID Certificates :

Revoked Certificates : Not Yet Valid Certificates :

Expired Certificates : Issuer Unknown :

Validation Response Expired : Others :

Name	Serial No.	Revoked	Expired	Issuer U...
Dr Evil	1A64228100000A74	X		
etisalat	010A		X	X
Hans Solo Expired	724FAFA330F1433A4...		X	X
REvokedCErTL10	08CA81D600000A4F	X		
Terminator1 From the Fu...	04BB873500000016			
Terminator2 From the Fu...	04BA98C700000015			
TL60GoodCert	0E			X

The following table lists and briefly describes the fields that can display in the dialog box.

Field	Description
No. of Certificates	Number of certificates associated with entries in your Address Book application
No. of Valid Certificates	Number of valid certificates (as determined by the Address Book Validator) in your Address Book application.
No. of INVALID Certificates	Number of invalid certificates (as determined by the Address Book Validator) in your Address Book application.
Revoked Certificates	Number of certificates that have been revoked.
Expired Certificates	Number of certificates that have expired.

Validation Response Expired	Number of certificates whose validity could not be determined because the CRL or CRT used to determine the validity of the certificate has expired.
Not Yet Valid Certificates	Number of invalid certificates whose validity date is in the future.
Issuer Unknown	Number of certificates whose issuer is unknown to the Address Book Validator.
Others	Number of certificates determined invalid for other reasons, such as the certificate being corrupted.

- Step 3 Click **Details** to view a list of the invalid certificates, which includes the certificate owner, certificate serial number, and validation status.

Adding Trusted Root Certificates

To verify the status of a digital certificate used to sign an email, the Validator must trust the certificate. A certificate is trusted if the root certificate of the Certification Authority (CA) that signs the certificate is known to the Validator. For a CA to be known to the Validator, the Root certificate of the CA must be stored in your Windows certificate store. This allows the Address Book Validator to trust the validation responses it obtains from the CA.

Your site administrator will tell you which certificates you need to obtain and where to get them.

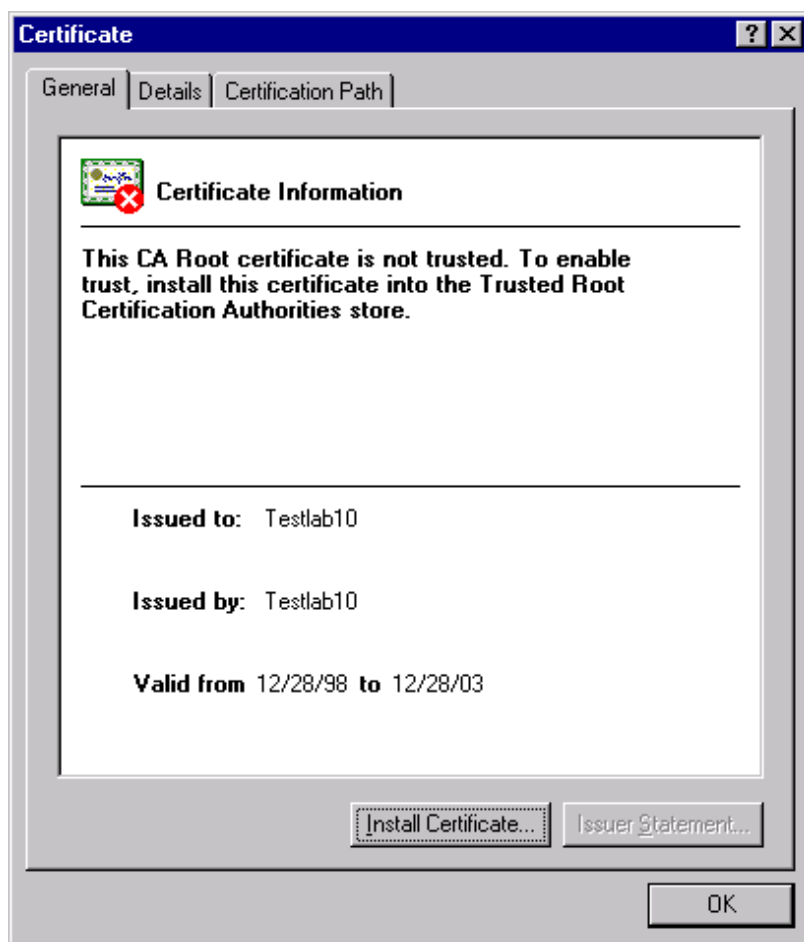


NOTE: You will need Internet Explorer 4.01 or later to add certificates, but version 5.0 or later is recommended.

To add a new certificate to your Windows certificate database

- Step 1 Get the certificate.
- Step 2 Double click on it.

The Certificate dialog displays.

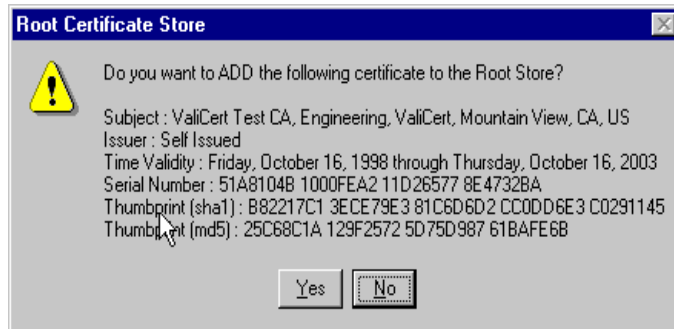


Step 3 Click **Install Certificate.**

The Certificate Manager Import Wizard launches.

Follow the instructions to import the certificate into the Windows certificate store.

In the last step, the following dialog displays to confirm that you want to add the certificate.



Step 4 Click **Yes to add the certificate to your certificate database.**

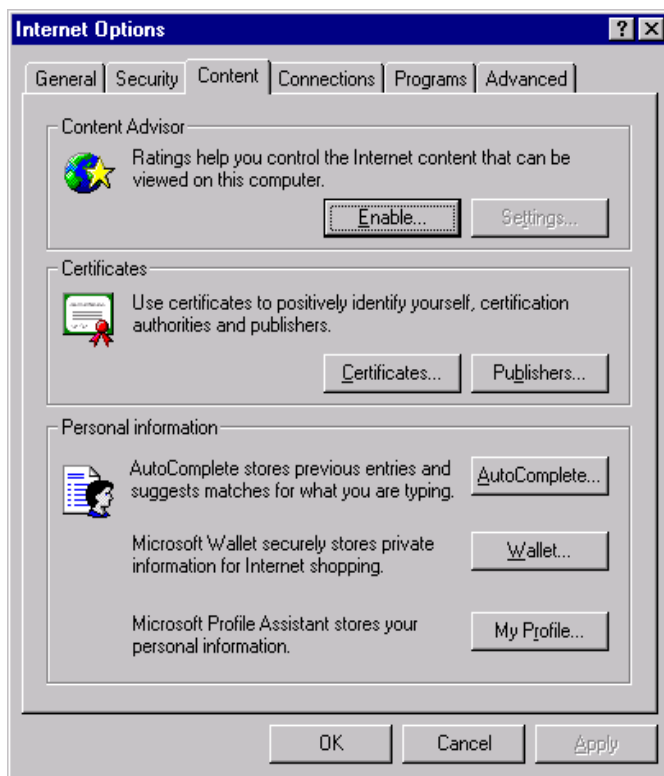
The certificate is added to your database.

To verify that you have added the certificate, and see which other certificates are in your certificate database:

Step 1 In Internet Explorer menu bar, select **Tools > Internet Options**.

Step 2 Select the **Content** tab.

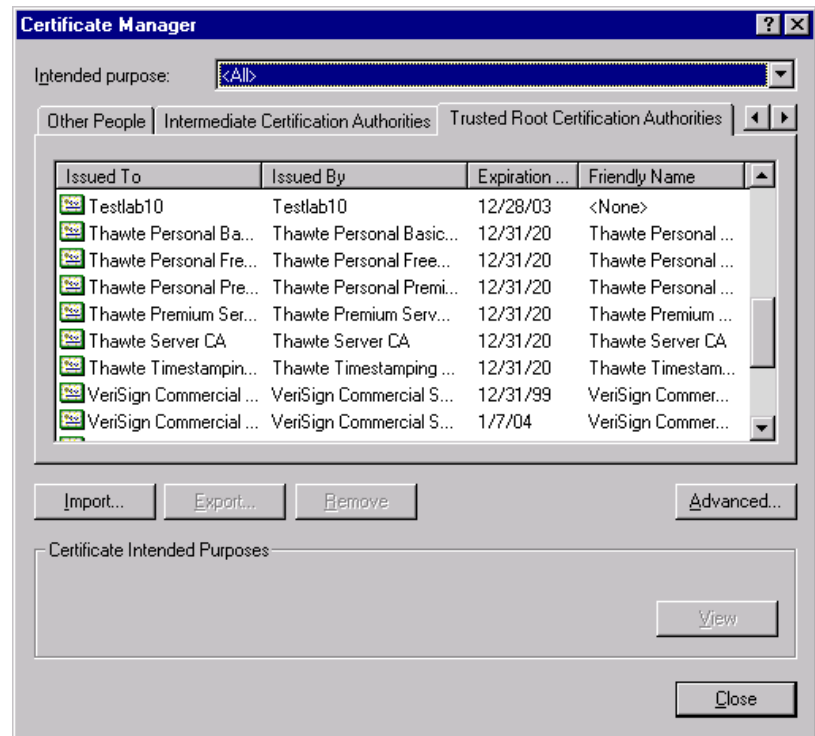
The following dialog box displays.



Step 3 Click **Certificates**.

Step 4 Select Trusted Root Authorities

The following dialog box displays.



- Step 5 Scroll through the listing of trusted CAs to confirm the certificate you added is in the list.

Sharing Contacts Address Book

By default, the Address Book Validator only looks at the certificates contained in the Windows Address Book. However, you can configure the Address Book Validator to look at the certificates of the contacts you added in your Contacts Address Book.

Under **Options** in the Explorer Address Book (which is also the Windows Address Book), click the radio button to enable sharing with Contacts in Outlook Address Book.



NOTE: If this does not work, manually download the certificates into your Address Book.

Certificates must be in the DER format.

When sharing is enabled, the Address Book Validator will look at certificates of the contacts that were added from Outlook.

Creating the CRL Initialization File

If you are using CRLs to validate certificates, you might need to create or edit an initialization file that contains information about the CRLs. Your site administrator may have provided you with such a file.

To create or edit the file, use the following format for each CRL.

```
VC_CA_<ca_number>_PUB_KEY_HASH=<hash>
VC_CA_<ca_number>_CRL_TYPE=<crl_type>
VC_CA_<ca_number>_CRL_URL=<crl_url>
```

The following table lists and briefly describes each of the variables:

Variable	Description
ca_number	Number of the entry in the file. For example, 1 for the first CA listed, 2 for the second, and so forth.
hash	Public key hash of the CA certificate. You can get this from your site administrator or by using the <code>dumppubkeyhash.exe</code> program.
crl_type	CRL Type. The value 0 specifies DER-encoded (binary) CRLs and 1 specifies base-64-encoded (ASCII) CRLs.
crl_url	LDAP or HTTP URL of the CRL.

The following is an example of an entry:

```
VC_CA_1_PUB_KEY_HASH=082917F8CFE82DFCEBE23B94769377285E9F81DE  
VC_CA_1_CRL_TYPE=0  
VC_CA_1_CRL_URL=http://bravo/CertSrv/bravo.crl
```


Using Validator for Microsoft IIS

The ValiCert Web Server Validator is a filter for Microsoft IIS that ensures that your Server does not accept invalid certificates during secure web connections. This section helps you to configure and use your web server (Microsoft IIS) and the Web Server Validator for Microsoft IIS.

The following tasks are described:

- ❖ Configuring Your Web Server
- ❖ Customizing the Error Page
- ❖ Using CRLs for Validation
- ❖ Editing the Configuration File
- ❖ Using the Web Server Validator

Configuring Your Web Server

After you have installed the Web Server Validator, you need to configure your web server (Microsoft IIS or PWS) so that it will use the Validator.

To configure your web server

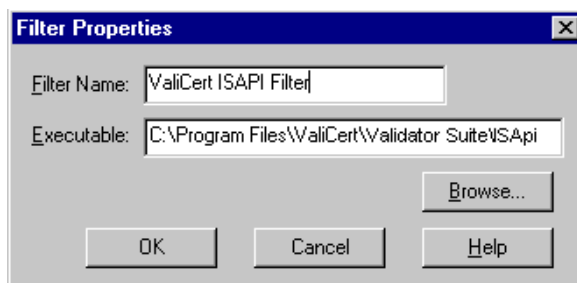
- Step 1 Click on your workstation name under **Internet Information Server** in the Internet Service Manager application.
- Step 2 Right click on the name of the Web site where you want to install the Web Server Validator, then select **Properties** from the pop-up list that appears.
- Step 3 Select the **ISAPI Filter** tab in the Properties dialog box.
- Step 4 Click **Add**.
- Step 5 Type the name of the filter (this can be any name you want) in the **Filter Name** box.

Step 6 Type the full path of the `vcisapi.dll` in the **Executable** text field.



NOTE: The default path of the `vcisapi.dll` is:

`<VCInstallDir>\ISAPI\vcisapi.dll`



Step 7 Click **OK**.

Customizing the Error Page

The Validator displays an HTML error page when it encounters an error. An error can occur when the Validator encounters an expired certificate, cannot reach the VA, or encounters a CA who is unknown an error page is displayed. This page can be customized to display any message. You can replace the page template or gif file to display when an error occurs.

To customize the page edit the parameters in the `[CUSTOMIZATION_SECTION]` of the configuration file `vcisapi.ini`. Edit the messages or specify a new HTML template or gif file for the error page.

Using CRLs for Validation

If you want the Web Server Validator to use CRLs when validating certificates edit the variables in the `[CRL_SECTION]` of the configuration file `vcisapi.ini`. For each CRL that is providing CRL information, specify the CA's public key hash, CRL type and URL. Create these entries for each CRL, and number the entries sequentially.

To configure the Validator to use CRLs to validate certificates

Edit the initialization file `vcisapi.ini`. Create an entry in the following format for each CRL.

```
VC_CA_<ca_number>_PUB_KEY_HASH = <hash>
VC_CA_<ca_number>_CRL_TYPE = <crl_type>
VC_CA_<ca_number>_CRL_URL = <crl_url>
```

<ca_number> represents the number of the entry in the file, that is, 1 for the first CA listed, 2 for the second, and so forth.

<hash> is the public key hash of the CA certificate. You can get this from your site administrator or by using the `dumppubkeyhash` program (located in <VCInstallDir>\ISapi\ directory).

<crl_type> is 0 for DER-encoded CRLs and 1 for base-64-encoded CRLs.

<crl_url> is the LDAP or HTTP URL of the CRL.

The following is an example of a CRL entry:

```
VC_CA_1_PUB_KEY_HASH=082917F8CFE82DFCEBE23B9476937
7285E9F81DE
VC_CA_1_CRL_TYPE=0
VC_CA_1_CRL_URL=http://bravo/CertSrv/bravo.crl
```

Editing the Configuration File

To configure the Validator, edit the initialization file `vcisapi.ini`. The file is divided into sections based on functionality. When you make changes to the ini file, they will take effect for the next validation request. You do not need to re-start the web server.



NOTE: On startup, the Validator looks for the `vcisapi.ini` file in the installation directory.

Each entry in the `vcisapi.ini` file is a name-value pair, separated by an equal sign (=), except for section names which stand alone.



NOTE: To enable an entry in the ini file, remove pound sign (#) at the beginning of the line

You can configure general controls of the Validator, the VA that is accessed for validation, the CRL information and the error reporting page.

The following are the parameters in the configuration file.

Table 1. vcisapi.ini Parameters

Variable	Definition	Default Value
[GENERAL_SECTION]	This section that contains general Validator parameters.	
VC_TIME_SKEW	The amount of time (in seconds) that the clock of another machine that communicates with the Validator host can differ. NOTE: This is provided as a work around when sync up is not available.	300
VC_LOG_FILE	The name of the log file, specified as the complete path.	<VCInstallDir>\vcisapi.log
VC_LOG_LEVEL	The level of logging. Set to 0 for Warning and Errors only or 1 for detailed logging.	0
VC_USE_PROXY	Determines whether to use a proxy server or not. Set to 0 for no proxy server or 1 to use a proxy server.	0
VC_PROXY_HOST	To use a proxy server specify the host.	None
VC_PROXY_PORT	To use a proxy server specify the port.	None
VC_VALIDATION_MECHANISM	This determines the validation protocol the Validator uses. Set to 0 for CRT, 1 for OCSP, and 2 for CRL.	0
[VA_SECTION]	This section contains parameters that pertain to the VA.	
VC_VA_CERT	The path of the VA root certificate file.	None
VC_VA_CERT_TYPE	This specifies the encoding of the certificate. Set to 0 for DER or 1 for BASE64.	1

Table 1. vcisapi.ini Parameters

VC_VA_URL	The URL of the VA that issues validation information.	None
[CRL_SECTION]	This section contains the general parameters that pertain to CRLs. For each CA issuing CRLs include the following three parameters where <n> is the number of each CA listed, 1 for the first CA listed, 2 for the second and so forth.	
VC_CA_<n>_PUB_KEY_HASH	The hash (in hex) of the public key for the CA. To get this use the dumppubkeyhash.exe program.	None
VC_CA_<n>_CRL_TYPE	This specifies the encoding of the CRLs from the CA. Set to 0 for DER or 1 for BASE 64.	1
VC_CA_<n>_CRL_URL	The LDAP or HTTP URL of the CRL.	
VC_CERT_CHAIN_CHECK	This specifies whether the client certificate will be checked or the whole certificate chain. Set to 0 to only check the client certificate, or to 1 to check the whole chain.	0
[CUSTOMIZATION_SECTION]	This section contains parameters that pertain to customizing the error reporting page.	
VC_STR_REVOKED	The error message that displays when the certificate is revoked.	Certificate Has Been Revoked
VC_STR_VR_EXPIRED	The error message that displays when the validation response has expired.	Validation Response Has Expired
VC_STR_VR_NOT_ACTIVATED	The error message that displays when the Validation response is not yet valid.	Validation Response Is Not Activated
VC_STR_ISSUER_NOT_TRUSTED	The error message that displays when the certificate is unknown to the VA. (The CA's root certificate is not in the VA's certificate store.)	Certificate Issuer Is Not Trusted by the VA
VC_STR_VA_NOT_TRUSTED	The error message that displays when the VA is unknown to the Validator. (The VA's root certificate is not in the web server's certificate store.)	Validation Issuer Is Not Trusted
VC_STR_INTERNAL_ERROR	The error message that displays when there is an error in the data.	Data Related Error
VC_STR_CERT_CHAIN_NOT_CONSTRUCTED	The error message that displays when the certificate chain cannot be constructed.	Certificate Chain could not be constructed

Table 1. vcisapi.ini Parameters

VC_STR_VA_UNREACHABLE	The error message that displays when the VA is unavailable, (the Validator can not connect).	Cannot connect to the Validation Authority
VC_STR_CRL_NOT_AVAILABLE	The error message that displays when a CRL is not available (when using CRL validation).	Revocation Information Is Not Available
VC_ERROR_TEMPLATE	The full path of the HTML template for the error page.	<vcisapi install directory>/template_vcisapi.html
VC_STR_STOP_GIF	The full path of the GIF file that displays on the error screen.	/valicert/stop.gif

Using the Web Server Validator

After you install and configure the Web Server Validator, it will automatically validate client certificates for Secure HTTP (HTTPS) requests. The Web Server Validator validates the following:

- ❖ Certificates from CAs that have registered with the ValiCert Global VA Service.
- ❖ Certificates issued internally if the CA has been configured to publish revocation data to your VA server.
- ❖ Certificates issued by CAs whose CRL information is specified in the CRL section of the initialization file.

CHAPTER 7

Using Validator for Netscape Server

The ValiCert Web Server Validator is a plug-in that ensures that your Netscape Enterprise Server (NES) does not accept revoked certificates during secure web connections. This section describes how to configure and use the ValiCert Web Server Validator for Netscape.

By default, the Web Server Validator is configured to use the ValiCert Global VA Service via the CRT protocol.

The following tasks are described:

- ❖ Editing the Configuration File
- ❖ Configuring Validator to use CRLs
- ❖ Configuring Validation Caches
- ❖ Configuring Validation Caches
- ❖ Customizing Validator Output
- ❖ Using the Web Server Validator

Editing the Configuration File

To configure the Web Server Validator edit the configuration file `vcnsapi.ini`. The default location of the `vcnsapi.ini` file is:

```
<server instance dir>/config/ValiCert/vcnsapi.ini
```

Each entry in the `vcnsapi.ini` file is a name-value pair, separated by an equal sign (=), except for section names which stand alone.



NOTE: To enable an entry in the ini file, remove pound sign (#) at the beginning of the line

The following table describes each of the parameters that you can edit in the `vcnsapi.ini` file.

The following are the parameters in the configuration file.

Table 2. vcnasapi.ini Parameters

Variable	Definition	Default Value
VC_NS_CERT_DB	Location of the Netscape certificate database needed for CRT, OCSP, and CRL validation. This database is usually under the alias folder in the Netscape Enterprise Server installation.	None.
VC_TIME_SKEW	The amount of time (in seconds) that the clock of another machine that communicates with the Validator host can differ. NOTE: This is provided as a work around when sync up is not available.	300
VC_LOG_FILE	The path of the ValiCert Web Server Validator log file.	<nes server install directory>/ vcnsapi.log
VC_LOG_LEVEL	The level of logging messages. Set to 0 for warning/error messages or 1 for informational messages NOTE: Specifying 1 generates large log files.	0
VC_USE_PROXY	This parameter specifies whether to use a proxy server for CRL, OCSP, and CRT downloads. Set to 0 to not use proxy server or 1 to use proxy server,	0
VC_PROXY_HOST	For CRL downloads, this parameter specifies the proxy host name for HTTP over proxy, if applicable.	None.
VC_PROXY_PORT	For CRL downloads, this parameter specifies the proxy port number for HTTP over proxy, if applicable.	None.
VC_VA_CACHE_SIZE	Memory cache size (in number of certificate validation responses).	100

Table 2. vcnasapi.ini Parameters

VC_VA_CACHE_DURATION	Duration, in seconds, that a validation response is cached in memory.	The default is to cache each validation response entry until it expires. The expiration time is determined by the nextUpdate value in the VA response.
VC_VA_RESP_LIFESPAN	Expiration time (in seconds) of a validation response when the validation response contains no expiration time related information.	60
VC_CRL_CACHE_DIR	Directory location for caching the CRL.	<nsapi install directory>/config/crlcache
VC_CRL_CACHE_DURATION	Maximum cache duration of CRLs, in seconds.	The default cache duration is until the CRL expires.
VC_VALIDATION_MECHANISM	Validation mechanism to use. Set to 0 for CRT, 1 for OCSP, or 2 for CRL.	0
VC_GVAS_OR_EVA	This specifies the type of VA for CRT/OCSP based validation. Set to 0 to use Global VA Service or 1 to use a local (Enterprise) VA.	0
VC_GVAS_CERT	For CRT/OCSP based validation, the location of certificate for ValiCert Global VA Service. NOTE: Use this parameter only to override the certificate embedded in the software.	
VC_GVAS_CERT_TYPE	The encoding method of the ValiCert Global VA Service certificate. Set to 0 for DER or 1 for Base-64.	
VC_GVAS_URL	URL for the ValiCert Global VA Service issuing CRT/OCSP responses.	For CRT: http://ci.valicert.net/ For OCSP: http://ocsp.valicert.net/.
VC_EVA_CERT	For CRT/OCSP based validation, this parameter specifies the location of certificate of local Validation Authority.	None.

Table 2. vcnasapi.ini Parameters

VC_EVA_CERT_TYPE	Encoding method used for ValiCert Enterprise VA certificate. Set to 0 for DER or 1 for Base-64.	1
VC_EVA_URL	The URL of the local Validation Authority issuing CRT or OCSP responses.	None.
VC_CA_<n>_PUB_KEY_HASH	Hash (in Hex) of public key for CA <n> where <n> is the number of each CA listed.	None.
VC_CA_<n>_CRL_TYPE	For each CA issuing CRLs include these first three parameters where <n> is the number of each CA listed, 1 for the first CA listed, 2 for the second and so forth. The encoding of the CRL issued by CA <n>. Set to 0 for DER, 1 for Base 64 or 2 for Hex. NOTE: Only DER is valid for HTTP.	1
VC_CA_<n>_CRL_URL	The HTTP or LDAP URL for downloading CRLs from CA <n> (where <n> is the number of each CA listed).	None.
VC_CERT_CHAIN_CHECK	This specifies whether the client certificate will be checked or the whole certificate chain. Set to 0 to only check the client certificate, or to 1 to check the whole chain.	0
VC_STR_REVOKED	The error message that displays if a certificate is revoked.	Certificate Has Been Revoked
VC_STR_VR_EXPIRED	The error message that displays if a validation response has expired.	Validation Response Has Expired
VC_STR_VR_NOT_ACTIVATED	The error message that displays if a Validation Response is not yet valid.	Validation Response Is Not Activated
VC_STR_ISSUER_NOT_TRUSTED	The error message that displays if a CA is not trusted by a VA.	Certificate Issuer Is Not Trusted by the VA
VC_STR_VA_NOT_TRUSTED	The error message that displays if a VA is not trusted.	Validation Issuer Is Not Trusted
VC_STR_INTERNAL_ERROR	The error message that displays when the Web Server Validator encounters errors that cannot be resolved by users.	Data Related Error
VS_STR_CERT_CHAIN_NOT_CONSTRUCTED	The error message that displays when a Certificate Chain cannot be constructed by the Web Server Validator.	Certificate Chain could not be constructed

Table 2. vcnasapi.ini Parameters

VC_STR_VA_UNREACHABLE	The error message that displays if the ValiCert Web Server Validator cannot connect to the Validation Authority to obtain the status of a certificate.	Cannot connect to the Validation Authority
VC_ERROR_TEMPLATE	Template of the HTML page that displays for error messages when a certificate is revoked or is invalid.	<nsapi install directory>/template.html
VC_STR_STOP_GIF	The full path of the GIF file that displays next to a negative assertion on the error page.	/valicert/stop.gif

Configuring Validator to use CRLs

To configure the Web Server Validator to use CRLs

Step 1 Identify the Netscape certificate database (<certificate_db>).

The following is an example:

```
<server>/alias/<server instance alias>-cert*.db
```

Step 2 Dump the hashes of the public keys of all the certificates in the certificate database into a file.

The ValiCert `dumpCAHash` program (<server instance dir>/config/ValiCert/dumpCAHash) dumps the public key hashes into the specified file. The default dump file is `vcnsapi.out`

The `dumpCAHash` program takes the certificate database file as its input parameter and dumps the hashes to the file specified by the `-o` option.

For Windows NT, enter the following at the command line:

```
dumpCAHash.exe [ -o <output_file> ]  
<certificate_db>
```

For UNIX, enter the following at the command line:

```
dumpCAHash [ -o <output_file> ] <certificate_db>
```

The output file contains an entry for each CA certificate in the certificate database. Each entry is made up of a hash of the public key and a description of the CA to which the public key belongs. To

select the CRL for a CA, you will need to specify the hash portion of the entry in the `VC_CA_<n>_PUB_KEY_HASH` parameter. See Step 4.

The following is an example of a hash of a public key contained in the output file:

```
F5ED1D418453EB5B8177CDD951FBC52E8F42CE8A
```

- Step 3 The value of the `VC_NS_CERT_DB` variable to your server's Netscape certificate database is set during installation. To change the database, edit the following variable:

```
VC_NS_CERT_DB
```

- Step 4 For each CA you must create entries in the ini file. Number the certificate's variables sequentially. For example set the values of the `VC_CA_1_PUB_KEY_HASH`, `VC_CA_1_CRL_TYPE`, and `VC_CA_1_CRL_URL` variables for the first CA that you need to set up for validation.

The `VC_CA_1_PUB_KEY_HASH` value can be found in the `<vcnsapi.out>` file generated in step 2.

The following is an example of an entry in the `vcnsapi.ini` file:

```
VC_CA_1_PUB_KEY_HASH=F5ED1D418453EB5B8177CDD951FBC52E8F42CE8A
VC_CA_1_CRL_TYPE=1
VC_CA_1_CRL_URL=http://www.test1.com/CRLs
```



NOTE: Set up similar variables for each CA from which you want to obtain CRLs.

- Step 5 Set the value of the `VC_VALIDATION_MECHANISM` variable to 2. This value specifies that the Web Server Validator will use CRLs as the validation mechanism.
- Step 6 Restart the server instance.

Configuring Validation Caches

The Web Server Validator provides two separate, configurable validation caches. The caches are:

- ❖ The CRL cache
- ❖ The Validation Response cache

Both caches reside locally on the Web Server Validator. However, the CRL cache resides on disk while the Validation Response cache resides in memory.

The CRL cache is used to maintain local validation information (if using the CRL validation mechanism) for CAs. The Validation Response cache is used to maintain local validation information for all certificate validation requests, regardless of the validation mechanism used.

Configuring the CRL Cache

The CRL cache contains CRLs that have been downloaded from CAs. The CRL cache only contains CRLs from CAs specified in the following parameters in the `vcnsapi.ini` file:

- ❖ `VC_CA_<n>_PUB_KEY_HASH`
- ❖ `VC_CA_<n>_CRL_TYPE`
- ❖ `VC_CA_<n>_CRL_URL`

When the Web Server Validator receives a CRL, it places the CRL in its own separate directory in the directory that you specify in the `VC_CRL_CACHE_DIR` parameter. The default directory under which each CRL directory is placed is `crlcache` which can be found under the `<server instance dir>/config` folder.

The directory structure would look similar to the following:

```
crlcache/<CA1IDdir>/latest.crl  
crlcache/<CA2IDdir>/latest.crl  
crlcache/<CA3IDdir>/latest.crl
```



NOTE: You can only specify a replacement value for `<server instance dir>/config/crlcache`. How each CRL is cached under that directory is determined by the Web Server Validator. This means you do not have control of how the CRLs are cached in their separate directories.

In addition to specifying the CRL cache directory, you can specify the length of time that the CRL can reside in the CRL cache. The default is to cache the CRL until it expires.

To configure the CRL cache

Step 1 Configure the CRL cache directory.

Define a value for the `VC_CRL_CACHE_DIR` parameter or use the default value, `crlcache`.

Step 2 Configure how long the CRL will be cached.

Define a value for the `VC_CRL_CACHE_DURATION` parameter or use the default value, until the CRL expires.



NOTE: If the CRL does not contain a duration value, the value of the `VC_VA_RESP_LIFESPAN` parameter is used. The default value for this variable is 60 seconds.

Configuring the Validation Response Cache

The Validation Response Cache contains responses to all validation requests that have been made. The cache maintains an entry for each client certificate. Each entry contains an identifier for the certificate validated, the status of the certificate, and an expiration time for the entry. If the status expiration time is different from the duration time specified for the cache, the lesser of the two values will be used as the entry expiration time.

To configure the Validation Response cache

Step 1 Specify how long to cache the response in memory.

Set a value for the `VC_VA_CACHE_DURATION` parameter in the `vcnsapi.ini` file. Duration, in seconds, that a validation response is cached in memory. The default is to cache each validation

response entry until it expires. The expiration time is specified in the VA response.

- Step 2 Specify the size of the Validation Response cache you want the Web Server Validator to maintain in memory.

Set a value for the `VC_VA_CACHE_SIZE` parameter in the `vcnsapi.ini` file. The size is in number of certificate validation requests that are cached. The default is 100 responses. Once this size is exceeded, the response is written over, regardless of the duration you have specified.

Customizing Validator Output

You can customize the output page the end-user's browser displays as the Web Server Validator validates certificates. In addition, you can modify the error messages, as well as change the status icons that appear on this page.

To customize the page, edit the existing template or specify an alternate template.

To customize the Validator output page

- ❖ Edit the template file.

On UNIX, edit the following file:

```
<server instance dir>/config/ValiCert/template.html
```

On Windows NT, edit the following file:

```
<server instance dir>/config/template.html
```

- ❖ On Windows NT,

Alternatively, create your own file whose name and location you specify with the `VC_ERROR_TEMPLATE` parameter in the `vcnsapi.ini` file.

To display different icons on the output page

- ❖ Edit the values for the following parameters in the `vcnsapi.ini` file.

`VC_STR_STOP_GIF`

To modify the error messages displayed on the output page

- ❖ Edit the value for the following parameters in the `vcnsapi.ini` file.

`VC_STR_REVOKED`
`VC_STR_VR_EXPIRED`
`VC_STR_VR_NOT_ACTIVATED`
`VC_STR_ISSUER_NOT_TRUSTED`
`VC_STR_VA_NOT_TRUSTED`
`VC_STR_INTERNAL_ERROR`
`VS_STR_CERT_CHAIN_NOT_CONSTRUCTED`
`VC_STR_VA_UNREACHABLE`

Using the Web Server Validator

After you have installed and configured the Web Server Validator for Netscape Enterprise Server, it will automatically validate client certificates for secure HTTP requests. The Web Server Validator can only validate certificates from CAs that have signed up with the ValiCert Global VA Service or from any CA trusted by both the VA and web server at your site.

The stop sign icon conveys a negative status for the corresponding validation check.



NOTE: Messages and icons displayed on this page may vary, depending on whether the values in the `vcnsapi.ini` file have been changed.

Using the Browser Validator

The ValiCert Browser Validator is a module that enables your Internet Explorer browser to use a VA, or certificate revocation lists (CRLs) to validate server certificates in SSL connections and signed files downloaded from the Internet (files signed with Authenticode). After you have installed the ValiCert Browser Validator, you can validate signed files that you have downloaded from the Internet using http or ftp.

This section describes how to:

- ❖ Configure your Web browser
- ❖ Validate signed files

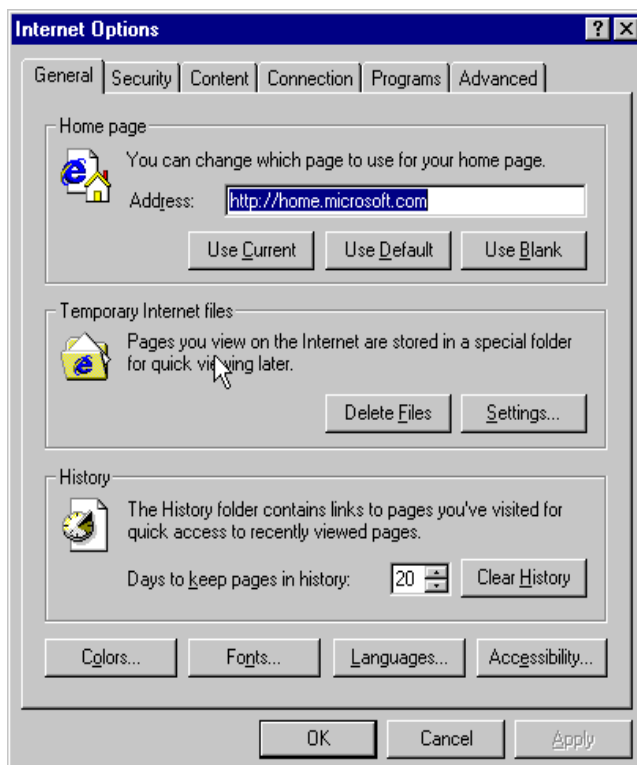
The ValiCert Browser Validator supports Microsoft Internet Explorer 4.0 and Microsoft Internet Explorer 5.0. (5.0 is recommended).

To configure your Web browser

Step 1 Launch the browser.

Step 2 Select **Internet Options** from the **Tools** menu.

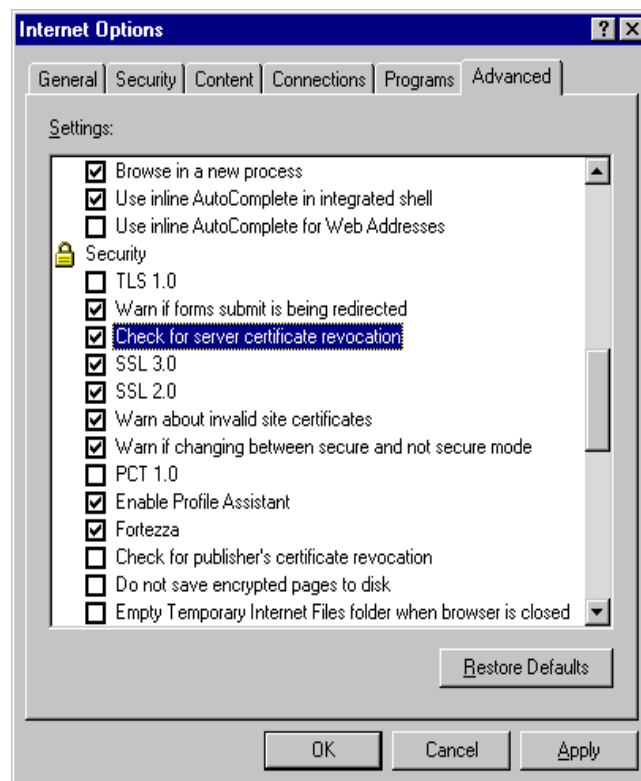
The Internet Options dialog appears:



Step 3 Click the Advanced tab.

Step 4 If using Internet Explorer 5.0, select the **Check for server certificate revocation** check box in the Security section. If using

Internet Explorer 4.0, select the **Check for server certificate revocation** check box in the Security section.

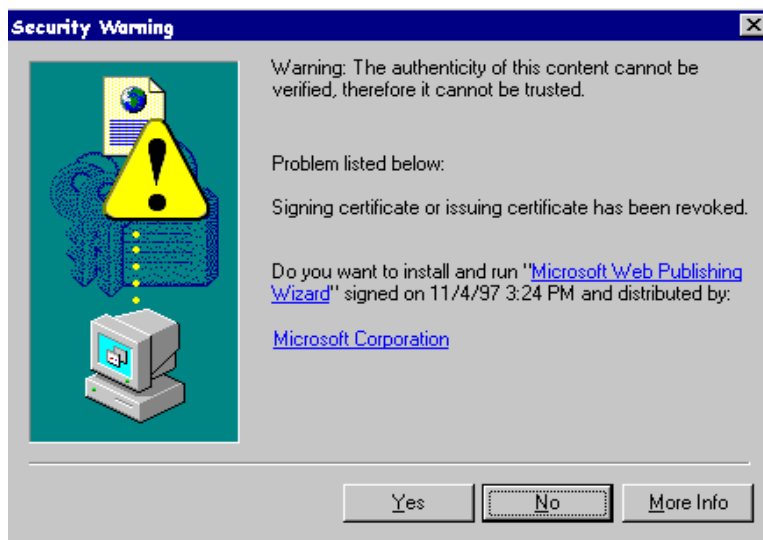


Step 5 Click **OK** to close the dialog box.

Your Internet Explorer browser will now use the ValiCert Global VA Service, ValiCert Enterprise VA, ValiCert Certificate VA, or certificate revocation lists to validate those files signed with Authenticode.

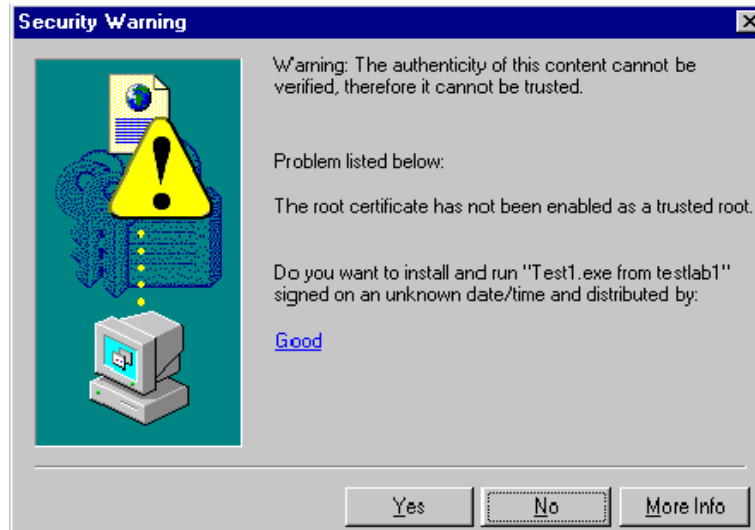
Validating Certificates

After installing the ValiCert Browser Validator, Internet Explorer will authenticate all certificates associated with files that you download via http or ftp, and server certificates in SSL. If the downloaded file is signed with an invalid certificate, Internet Explorer displays the following security warning:



If you attempt to download a file signed with a certificate from a CA that you have not trusted (either because you have not yet obtained the CA root

certificate, or you have explicitly decided not to trust certificates from this CA), Internet Explorer displays the following dialog box.



If a file is signed with a valid certificate, Internet Explorer displays a dialog box informing you that the certificate is valid; you can choose not to display this dialog in the future.



Using CRLs to Validate Certificates

In addition to using the ValiCert Global VA Service, ValiCert Enterprise VA, and ValiCert Certificate VA, the ValiCert Browser Validator lets you use certificate revocation lists (CRLs) to validate certificates used to sign files. To use CRL validation, you need to create a CRL initialization file (if your site administrator has not already provided you with one) and edit your registry so that your browser will use CRLs to validate certificates.

To configure your browser to use CRLs to validate certificates

Step 1 Create a CRL initialization file (typically named `vcCRL.ini`).

Step 2 For each CA that is publishing CRLs, create the following entries:

```
VC_CA_<n>_PUB_KEY_HASH=<hash>
```

```
VC_CA_<n>_CRL_TYPE=<crl_type>
```

```
VC_CA_<n>_CRL_URL=<crl_url>
```

The following table lists and briefly describes each of the variables:

Variable	Description
<n>	Number of the entry in the file. For example, 1 for the first CA listed, 2 for the second, and so forth.
<hash>	Public key hash of the CA certificate. You can get this from your site administrator or by using the <code>dumppubkeyhash</code> program.
<crl_type>	CRL encoding. Set to 0 for DER-encoded CRLs or 1 for base-64-encoded CRLs.
<crl_url>	LDAP or HTTP URL of the CRL

The following is an example of an entry:

```
VC_CA_1_PUB_KEY_HASH=082917F8CFE82DFCEBE23B94769377285E9F81DE
```

```
VC_CA_1_CRL_TYPE=0
```

```
VC_CA_1_CRL_URL=http://bravo/CertSrv/bravo.crl
```

Step 3 Use the registry editor to set the value of the following subkey to 2.

```
HKEY_CURRENT_USER\Software\ValiCert\Authenticode\3.2\
Validation Protocol
```

- Step 4 Set the value of the following subkey to the location of the CRL initialization file you just created.

```
HKEY_CURRENT_USER\Software\ValiCert\Authenticode\3.2\  
CRL_INI_FILE
```

- Step 5 Restart your Web browser.

CHAPTER A

Troubleshooting

This section provides solutions to problems encountered during the use of the ValiCert Validator Suite.

Email Validator

This section describes solutions to common problems you may encounter when using the Email Validator.

Problem: Dialog box reports Status Unknown for incoming messages.

Solutions:

Your VA does not recognize the CA that issued the certificates.

There is no CRL data available for the CA that issued the certificates --Your VA is offline or otherwise unavailable on the network.

Your Validator is unable to establish a network connection from your machine.

Your Validator is unable to construct a certificate chain; verify that any intermediate signing certificates are present on your system, in addition to the root certificate.

Your CRL has expired.

Problem: All my messages are reporting their status as Valid, even though I *know* I revoked one of my test certificates.

Solution: Be sure to force your CA to create a new CRL, and ensure that it is published to the VA.

Problem: The E-Mail Validator is functioning improperly.

Solution: If you have uninstalled and re-installed the E-Mail Validator to a different file path, be sure to reboot the machine after you re-install it.

Problem: Mail is Signed with the incorrect certificate.

Solution: If the certificate used to sign a mail has an e-mail entry which is different from the actual e-mail id of the mail client, Outlook actually tries NOT to use that particular certificate for signing. Outlook looks for certificates in it's certificate store that have the proper e-mail entry. In this case, the mail will be signed with some other certificate.

In this case you must get a new certificate for the client that has the correct email address.

Web Server Validator for Microsoft IIS

This section describes solutions to common problems you may encounter when using the Web Server Validator for Microsoft IIS.

Problem: Validation doesn't seem to be working

Solutions:

Verify the VA is accessible on the network.

Verify that the relevant ini file settings specify the full machine and domain name for your VA server.

Verify that the port number of your VA server as specified in the ini file is correct. If you are using multiple IP addresses on your IIS machine, make sure your Validator is not talking to port 80 for another server on one of the other IP addresses.



NOTE: Basic connectivity can be confirmed by checking the VA server "stats" page. If the Validator is correctly configured, the counts for the appropriate protocol will be incremented each time a secure page is hit.

Problem: My web browser does not list any client certificates to submit, even though I have them installed.

Solution: Verify that your IIS server has your CA's root certificate installed.

Problem: My web browser is not able to connect to the secure site. In addition, my web browser indicates that there are no certificates.

Solution: Verify that your IIS server is using Service Pack 3.0, 5 or above. There are known incompatibilities with Service Pack 4.0.

Web Server Validator for Netscape Enterprise Server

This section describes solutions to common problems you may encounter when configuring or using the ValiCert Web Server Validator for Netscape Enterprise Server.

Problem: The user cannot select a client certificate to use for authentication when connecting to your https server, (that is, Netscape Navigator displays a No User Certificate dialog box or Internet Explorer displays an empty Select Certificate dialog box.

Reason: Your web server does not trust any of the end-user's certificates.

Solution: If the CA that issued the client certificate is a trusted entity, you need to add its root certificate to your web server's certificate database.

Problem: You have made changes to the `vcnsapi.ini` file, but they have not taken effect.

Reason: The line you edited may still be commented out, or you did not restart the server instance after editing the file.

Solution: Ensure that you have removed the number sign (#) from the beginning of any lines you have edited, then restart the server instance.

Problem: Web Server Validator gives (status info unavailable) message.

Reasons:

- 1 The Enterprise VA does not trust the CA that issued the certificate you are checking.
- 2 The Enterprise VA does not have a CRL from the CA.
- 3 The Enterprise VA has an out-of-date CRL for the CA.

Solutions:

- 1 Add the CA root certificate to the Enterprise VA.
- 2 Generate and publish a new CRL from the CA to the VA.
- 3 Generate and publish a new CRL from the CA to the VA.

Problem: Validation does not seem to be working

Solutions:

- ❖ Verify the `obj.conf` for the relevant server instance is correctly configured.
- ❖ Verify the VA is accessible on the network.
- ❖ Verify that the port number of your VA server as specified in the `vcnsapi.ini` file is correct.
- ❖ If you are using multiple IP addresses on your NES machine, make sure your Validator isn't talking to port 80 for another server on one of the other IP addresses.
- ❖ Change the log file level and check the log file specified in the `vcnsapi.ini` file.

Problem: My web browser does not list any client certificates to submit, even though I have them installed.

Solution:

- ❖ Verify that your NES server has your CA's root certificate installed.

Index

A

- activity log
 - configuring 42
 - path and name 44
 - size 44
 - tab 43
- address books
 - configuring 48
 - contacts 57
 - tab 48
- address books, supported 2
- advanced tab 78
- alerts
 - audio 45, 46
 - checking interval 46
 - configuring 44, 45
 - for invalid certificates 44
 - frequency 46
 - tab 45
 - visual 45
- audience vii
- audio alert 45, 46
- authenticode 77, 79

B

- browsers supported 4, 77

C

- CA
 - certificate issuer type 30
 - verifying certificate 28
- CA root certificate, not yet obtained 80
- cache
 - CRL directory 69

certificate

- not trusted 80
- revoked 34
- unknown issuer 36
- unknown status 36
- Certificate Authorities dialog box 30
- Certificate Authority
 - see CA
- Certificate Chain
 - string 70
- Certificate Revocation List
 - see CRL
- certificate revocation lists
 - see CRLs
- Certificate Revocation Tree protocol
 - see CRT
- Certificate Validation Options dialog box 21
- certificate, invalid 80
- certificates
 - adding, IE required version 25, 53
 - catchall category 44
 - checking status 2
 - database 53
 - expired 44
 - invalid 53
 - issuer type 30
 - issuer unknown 44
 - not yet valid 44
 - response expired 44
 - revoked 43
 - status 51

- trusted root 25
- verifying 28
- certificates, validating 3
- checking status of certificates 2
- communicating with proxy server 46, 47
- configuration parameters 68
- configuring
 - caches 73
 - ISAPI filter 61
 - validating entity 22
 - validation response cache 74
 - validator to use CRLs 71
 - web server 61
- configuring validators to use 71
- connection
 - settings
 - to proxy server 47
- connection settings
 - to proxy server 46
- Contacts address book 57
- conventions, typographical viii
- credits, other products used x
- CRL
 - caching directory 69
- CRL cache
 - configuring 73
- CRL initialization file 24, 58, 82
- CRL type 24, 58
- CRL type variable 24, 58, 82
- CRL URL variable 24, 58, 82
- CRL, validating protocol 23
- CRLs 24, 49, 58, 71
 - cache duration 69
 - proxy host for downloads 68
 - proxy port for downloads 68
 - type variable 63
 - URL for downloading 70
 - URL variable 63
 - validating 3
- CRT 49, 50
- CRT, validating protocol 23

CRT/OCSP based validation 69

D

- Departmental VA
 - message unverified 37
 - validating entity 22
- Destination Information dialog box 13
- document set ix
- dumpCAHash program 71
- dumppubkeyhash.exe 63

E

- e-mail messages
 - reading 33
 - receiving signed 33
 - sending signed 31
 - signed by revoked certificate 34
 - signed by unknown issuer 36
 - signed by unvknown status certificate 36
 - signed message summary 33
 - status icons 33
- encoding method 69
- Enterprise VA
 - message unverified 37
 - validating entity 22
- error message template 71
- events logging 43
- expiration for responses 44
- Expired Certs event 44

F

- files, types digitally signed 4
- frequency of alerts 46
- Freshness Proof stamp 2
 - attached 31
 - attaching to messages 23
 - handling 21
 - trusting 23

G

- Global VA Service
 - message unverified 37
 - URL 69
 - validating entity 22

I

- installing
 - procedure 10
 - selecting component 12
 - Validator Suite 9
- installing on UNIX
 - Validator 19
- internet options 55
- Internet Options dialog 78
- introduction 1
- ISAPI filter
 - component of validator 3
 - configuring 61
 - purpose 3
- issuer
 - type 30
 - unknown 33
- Issuer Unknown event 44

L

- local data store 49, 50
 - message unverified 38
 - validating entity 22
- log file location 68
- logging events 43

M

- MAPI store 2, 34
- Microsoft Authenticode web site 4
- Microsoft Certificate Server, page 26
- Microsoft Internet Information Server 3, 61
- Microsoft Windows Address Book 2, 48
- MIME attachment
 - Freshness Proof stamp 31
- monitoring events 42

N

- Netscape certificate database location 68
- Netscape Communications x
- Netscape Enterprise Server 3, 67
- Netscape Server Instance(s) dialog box 14

- Not Yet Valid event 44
- note, explanation of viii

O

- obj.conf file, modifications made 19, 20
- OCSP 49, 50
- OCSP, validating protocol 23
- Online Certificate Status Protocol
 - see OCSP
- opening Preferences 42
- operating system requirement 5, 8
- Others event 44
- outgoing messages 31
- Outlook
 - MAPI store 34
- Outlook Add-In Manager 31
- output page, customizing 75

P

- packages 19
- Personal Web Server 3, 61
- platforms supported 2
- Preferences dialog box 42
- pre-installation task 5
- pre-installation tasks 6, 8, 9
- privileges 8
- protocol
 - configuring 50
- protocols, supported 49
- proxy host name 68
- proxy port number 68
- proxy server
 - configuring connection settings 46, 47
 - IP address 47
 - network name 47
- public key hash 70
- public key hash variable 24, 58, 63, 82
- R**
- reading messages 33
- Readme file, viewing 18
- receiving messages 33

- revoked certificate 33, 34
- Revoked Certs event 43
- root 20
- root certificate store 25, 53
- RSA Data Security x

S

- S/MIME e-mail 1, 21, 25, 53
- Secure Sockets Layer (SSL) 6, 8
- security warning 80
- self-signed certificate 50
 - encoding method 69
 - location 69
- Service Pack requirement 8
- service pack requirement 5
- Setup Complete dialog box 18
- signed e-mail
 - reading 2
 - receiving 1
 - sending 2
- signed files, validating 77
- smime.vfs attachment 32
- Solaris software packages 19
- SSLeay software x
- Start menu, adding program to 18
- starting validator 39
- status, icons for depicting 33
- stopping validator 40
- support
 - getting technical assistance ix
 - platforms 2, 5, 8
- symbols viii
- system requirements 5, 7, 8

T

- technical support ix
- Time of Day 46
- troubleshooting 85, 86, 87
- typographical conventions viii

U

- unknown
 - issuer certificate 36
 - status certificate 36
- unverified message, reasons for 37

- upgrade 9
- URL
 - Global VA Service 69
 - VA 70

V

- VA
 - URL 70
- VAInstallDir ix
- ValiCert Global VA Service 49, 50
- ValiCert Validator Suite
 - components 9
 - dialog box 12
- valid certificate 33
- validating
 - certificates 3, 62
 - certificates, using CRLs 82
 - CRLs 3
 - digitally signed files 4
 - entity used 22
 - protocol to use 23
 - server certificates 4
 - signed files 77
- validating certificates 24, 50, 58
- validation
 - information 49
 - method 49, 50
 - settings, configuring 49
 - tab 49
- validation mechanism 69
- validation proof 1, 21
- validation protocol 82
- validation response cache
 - configuring 74
 - duration 69
- Validation Response Expired event 44
- validation response, lifespan 69
- Validation Status dialog box 52
- validator
 - configuring 21
 - options available 40
 - starting 31, 39

- stopping 31, 40
- vcCRL.ini 82
- vcCRL.ini file 50
- vcnsapi.ini
 - configuration parameters 68
 - sample entry 72
- vcnsapi.ini file
 - default location 67
 - editing 67
- VCVal.tar file 20
- verifying CA certificates 28
- viewing certificate status 51
- visual alert 45

W

- web browser, configuring 77
- Web Server Validator
 - components 3
 - configuration parameters 68
 - configuring caches 73
 - configuring to use CRLs 62
 - troubleshooting 85, 86, 87
 - using 66, 76